بسم الله الرحمن الرحيم

ترجمة محاضرات المقرر

"الأخلاقيات والقوانين المتعلّقة بالحدود الإلكترونية"

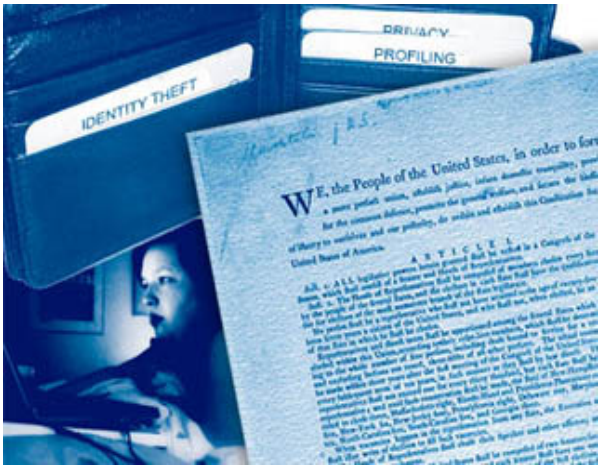
Ethics and the Law on the Electronic Frontier

- **فريق الترجمة:**

د. جميل إطميزي	**جامعة فلسطين الأهلية**	**فلسطين**	**j.itmazi@gmail.com**
ا. زهير خليف	**جامعة إنديانا**	**الولايات المتحدة الأمريكية**	**zuh.khlaif@gmail.com**

- **رابط المقرر الأصلي:**

https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-805-ethics-and-the-law-on-the-electronic-frontier-f



إن تنظيم الإنترنت له أصله في دستور الولايات المتحدة. وتستمر التكنولوجيا في تشكيل السياسات التي تحكم استخدام الحدود الإلكترونية .(صورة من MIT OpenCourseWare)

- محاضرون:

بروفيسور دانييل ويتزنر (Prof. Daniel Weitzner)

بروفيسور هارولد ابلسون (Prof. Harold Abelson)

بروفيسور مايكل م. فيشر (Prof. Michael M.J. Fischer)

- رقم المقرر بمعهد ماساتشوستس للتكنولوجيا (MIT): 6.805 / 6.806 / STS.085
- كما تم تدريسه في: خريف عام 2005م
- المستوى: المرحلة الجامعية

الاستشهاد كما ورد من المصدر:

Daniel Weitzner, Harold Abelson, and Michael Fischer. *6.805 Ethics and the Law on the Electronic Frontier*. Fall 2005. Massachusetts Institute of Technology: MIT OpenCourseWare, https://ocw.mit.edu. License: Creative Commons BY-NC-SA.

وصف المقرر:

يتناول هذا المقرر التفاعل بين القانون والسياسة والتكنولوجيا من حيث صلتها بالجدل الناشئ حول التحكم في الإنترنت. بالإضافة إلى ذلك، سيكون هناك معالجة متعمقة للخصوصية وفكرة "الشفافية"، واللوائح والتكنولوجيات التي تحكم استخدام المعلومات، وكذلك الوصول إلى المعلومات. والموضوعات التي يتم بحثها تشمل:

- الخلفية القانونية لتنظيم الإنترنت.
- قانون التعديل الرابع والمراقبة الإلكترونية.
- التنميط، واستخراج البيانات، وقانون الوطنية الأمريكية.
- التقنيات التي تخدم عدم الكشف عن الهوية والشفافية.
- التوعية بسياسة الويب.

الخطة الدراسية

رقم المحاضرة	**المواضيع**
1	نظرة عامة على الدورة والمقدمة صنع السياسة وهيكل القانون
الوحدة أ: تنظيم الإنترنت اللامركزي	
2	الإنترنت تلبي دستور الولايات المتحدة
3	تراث رينو (Reno): نقاط القوة والضعف للتصفية وتحكم المستخدم
الوحدة ب: تنظيم استخدام الحكومة لتقنية المراقبة	
4	أسس التعديل الرابعة والقرن الأول من المراقبة الإلكترونية
5	قضايا دولية
6	التحولات الحدودية العامة والخاصة القائمة على التكنولوجيا ملحق: حرب التشفير
7	التنميط والتنقيب في البيانات
الوحدة ج: تحدي الشفافية	
8	عدم الكشف عن الهوية مقابل الشفافية
9	المعلومات الشخصية على الويب
10	الشفافية في حماية المستهلك والتنظيم التجاري
11	أصول تنظيم البث
12	تحديات السياسة العامة على شبكة الويب الدلالية

محاضرات

"الأخلاقيات والقوانين المتعلّقة بالحدود الإلكترونية"

Ethics and the Law on the Electronic Frontier

توطئة:

مستخلص من واجبات المقرر المرافقة له / المترجم.

سوف يتعلق الجزء الأول بالحديث عن خلفية لوائح وتشريعات تنظيم الإنترنت، من حيث صلتها بالقانون الدستوري، ولا سيما فقه التعديل الأول المتعلق بحرية التعبير، وسيتم مقارنة الأساس القانوني لتنظيم الإنترنت مع وسائل الإعلام الأخرى، وخاصة الإذاعية، ثم يتم التركيز على قانون آداب الاتصالات وقرار المحكمة العليا في رينو ضد اتحاد الحريات المدنية (ACLU).

ثم ينتقل الحديث عن محاولات الحكومة لتنظيم المحتوى غير اللائق في المصدر، من خلال تفعيل قانون آداب الاتصالات لعام 1996. ونعلم أن الكونجرس ليس لديه السلطة لحظر هذه المواد والمحتويات غير اللائقة على الفور، وليس ليس لديه السلطة لاعتبار توفير هذه المواد للقاصرين عبر الإنترنت غير قانونية بشكل عام. ولكن هل تستطيع الحكومة فقط توفير الوصول المحدود (المفلتر) إلى الإنترنت؟ هل يمكن للحكومة أن تستخدم سلطتها لضمان أن يتم تحديد دخول القصر؟

ومن ثم سيتم التحدث عن أسس التعديل الرابع وأول جيل من المراقبة الإلكترونية، منتقلين من تأثيرات التعديل الأول لتنظيم خطاب غير لائق إلى التعديل الرابع وتداعيات الخصوصية للمراقبة الإلكترونية وعمليات البحث.

ومن ثم يتم الحديث عن الحدود الإلكترونية في أماكن مختلفة (قضايا دولية).

ثم يتم تناول التشفير (Cryptography) حيث ستتم بإجراء مراجعة / مسح لتكنولوجيا التشفير، ومن ثم نقاش محاولات الحكومة لتنظيم التشفير خلال تسعينيات القرن الماضي، بالإضافة إلى التطورات المتعلقة بالمخاوف بشأن استخدام الصوت عبر الإنترنت.

ثم ننتقل إلى التنميط بمعنى عمل سجلات بناء على تحليل صفات وخصائص والتنقيب في البيانات (Profiling and Datamining).

ثم يتم نقاش الشفافية في نقابل حق إخفاء الهوية

وبعد ذلك، يتم الحديث عن موضوع المعلومات الشخصية على شبكة الويب،

ثم الحديث عن موضوع الشفافية في حماية المستهلك والتشريعات التجارية

كيف يصبح المجاز (الاستعارة) قانونا: والحديث عن أصول تنظيم البث كمثال لكيفية فهم التكنولوجيا الجديدة أولاً من خلال الاستعارات؛ وفي حين أن الاستعارات قد تكون غير سليمة تقنياً، فإنها غالباً ما تشكل الأساس لقانون وتنظيم تلك التكنولوجيا.

ومن ثم يتم نقاش تحديات السياسة العامة على شبكة الويب الدلالية (Semantic Web).

محاضرة 1: نظرة عامة على المقرر والمقدمة
صنع السياسة وأسس القانون

غير متوفر من المصدر.

محاضرة 2: الإنترنت تتوافق مع دستور الولايات المتحدة

1994 – قدم السيناتور الأمريكي إكسون (Exon) جزاء من تشريع (القسم 223)،

ويغطي القسم 223 خدمات الاتصال الهاتفي (قانون اتصالات سيبل – Sable Communications Act) والمواد غير اللائقة وخدمات الاتصالات.
القانون انتهى أو سقط.

1995 – السيناتور إكسون أعاد تقديم القانون؛ وأعلن أيضا أنه يتقاعد، وإكسون أيضا مصوت رئيسي في لجنة الميزانية في مجلس الشيوخ وكان من حقه الحصول على التقاعد. (من جدول أعمال كلينتون). وجاء جدول أعمال السيناتور إكسون في وقت تشاركت فيه جدول أعمال أخرى.

وقد تم إقرار القانون المعروض تحت اسم "قانون آداب الاتصالات" (CDA) في الكونجرس الأمريكي، وهو يجرم إتاحة أي شيء غير لائق للأطفال أو إرسال أية مادة غير لائقة "بنية إزعاج الأطفال أو الإساءة إليهم أو تهديدهم أو التحرش بهم". / المترجم.

الجهات المعنية بقانون آداب الاتصالات (CDA):

- رابطة الكليات والجامعات الكاثوليكية (ACCU)،
- تنظيم الأسرة (Planned Parenthood)،
- جمعية المكتبات الأمريكية (ALA)،
- مزودو خدمة الإنترنت (ISP)،
- وشركات البرمجيات / الأجهزة.

الجهات التي دعمت مشروع هذا القانون:

1. الائتلاف المسيحي،
2. المجموعات المحافظة اجتماعيا.
3. مجلس بحوث العائلة (FRC)،
4. رابطة الأسرة الأمريكية (AFA).

وقد استغرق التصويت في مجلس الشيوخ فعليا ساعة واحدة، وقد صوت 84 لصالح حماية الأطفال من المواد الإباحية مقابل 16 صوتوا ضد حماية الأطفال من المواد الإباحية (يثير الدهشة).

علما انه في هذا العام (1995) ظهر المتصفح نيتسكيب (Netscape) للعموم.

في نفس الوقت، قام كريس كوكس ورون وايدن مع دعم نيوت غينغريتش في مجلس النواب والذي أخبر كريس كوكس لإيجاد طريقة مختلفة للتعامل مع المشكلة.

حيث تم صياغة اقتراح بديل يتجنب اتخاذ إجراءات عقابية ضد التعري من الملابس على الإنترنت والشتائم، وبدلاً من ذلك أكد على مبادرات التعليم الخاص للوالدين، وقد وافق مجلس النواب بأغلبية ساحقة على مشروع القانون ...، إلا أن المحكمة العليا رفضته في العام التالي في قضية رينو ضد ACLU. / المترجم.

وتم تقديم قانون إنترنت الأسرة وحرية التعليم (IFFEA) والذي يتضمن:

ا. السياسة – اتخاذ نهج تنظيمي وتمكين المستخدم،

ب. النتائج – إمكانات ديمقراطية، ولامركزية.

محاضرة 3: تراث رينو (Reno): نقاط القوة والضعف في تحكم المستخدم وفي الفلترة

غير متوفر من المصدر.

ملخص قضية رينو ضد الاتحاد الأمريكي للحريات المدنية / من المترجم:

كما أسلفنا، في عام 1996 أقرت إدارة الرئيس كلينتون قانون آداب الاتصالات (CDA) لحجب المضمون غير اللائق لحماية الأطفال الا ان المحكمة العليا للولايات المتحدة حكمت في 1997 بعدم دستورية هذا القانون في القضية (Reno v. ACLU) في عام وانه انتهك ضمان التعديل الأول لحرية التعبير، نظرا لصعوبة القيام بمنع المعلومات حتى وإن كانت هذه المعلومات تثير الشجب خوفا من ان يشكل ذلك حافزا لممارسة الرقابة على محتويات قد تكون مجرد مثيرة للجدل.

4 محاضرة: أسس التعديل الرابع والقرن الأول من المراقبة الإلكترونية

المحاضر: داني فايتزنر (Danny Weitzner)

التعديل الرابع:

خلال الأسابيع القليلة القادمة، سنركز على كيفية تبدّل التقنية وكيف ظهرت التكنولوجيا، وسننظر في أساسيات التعديل الرابع وقانون الاتصالات، كما وسنقوم أيضا بتدارس النشاط الخاص والنقاش حول تقنية التشفير.

{ **التعديل الرابع لدستور الولايات المتحدة الأمريكية** (Fourth Amendment): هو جزء من دستور الولايات المتحدة ومن وثيقة حقوق الولايات المتحدة. وهذا التعديل يمنع الحكومة من التفتيش والحجز من دون سبب، وأن الحكومة تحذر الفرد قبل قيامها بذلك. ويقول التعديل: لا يجوز المساس بحق الناس في أن يكونوا آمنين في أشخاصهم ومنازلهم ومستنداتهم ومقتنياتهم من أي تفتيش أو احتجاز من دون سبب، ولا يجوز إصدار مذكرة بهذا الخصوص إلا في حال وجود سبب معقول، معزز باليمين أو التوكيد، وتبين بالتحديد المكان المراد تفتيشه والأشخاص أو الأشياء المراد احتجازها }. إضافة من المترجم، من ويكيبيديا. [1]

والتعديل الرابع يمثل جزاء كبيرا من القانون. وفي معظم كليات الحقوق، يتم تغطية هذا الموضوع في ومقرر واحد أو عدة مقررات تتناول القانون الجنائي.

I. الخلفية التاريخية:

ا. في السابق، تم حل النزاعات القضائية من قبل الملك أو الملكة، ولكن هذا أصبح أمرا مرهقا جدا على الملك/ة.

ب. ثم تم تفويض المحاكم بموضوع النزاعات.

ج. حالة Semayne (حالة إنجليزية قديمة، 1604) –

(من المترجم: قضية قديمة تتناول كيفية تعامل الشريف أو العمدة في دخول البيوت وصلاحياته).

ملخص القصة: لم تكن هناك إجراءات، بل يجب أن يكون لمأمور المحكمة نوعًا من الإشعار (اليوم يسمى مذكرة قضائية) ويجب أن يؤسس هذا الإشعار على سبب معين (سبب محتمل). كما ويجب أن يتم الإعلان عن السبب الذي لأجله يتم التحقيق.

II. التعديل الرابع–4 أ (Fourth Amendment–4A)، يتضمن:

- إشعار (مذكرة قضائية)،
- السبب (دعوى محتملة)،
- إعلان (اطرق وأعلن)،
- الملكية (يشمل منزلك أو ملكيتك فقط)،

- تقصي/بحث عام أو سري.

- "قاضي مستقل ومحايد".

[1] من دستور الولايات المتحدة الأمريكية- جامعة منيسوتا، مكتبة حقوق الإنسان نسخة محفوظة 12 سبتمبر 2018 على موقع واي باك مشين.

كان البريطانيون دائمًا مهتمين بشأن التحقيق السري الذي يتم إجراؤه على هدف هذا التحقيق. فالتنصت على المكالمات الهاتفية هو موضوع مثير للاهتمام لأن وضع الآليات المذكورة أعلاه سيعرض أدلة التحقيق للخطر.

كانت فقرة (اطرق وأعلن) لصالح الشخص الذي يطلب منه ان يتم تفتيش ممتلكاته حيث يفترض أن الشخص سيفتح بابه طواعية.

هذه الأشياء الأساسية تشكل أساس التعديل الرابع، وهو قانون البحث والضبط.

والعمل الحقيقي في هذه الحالة يشير إلى الملكية الثابتة (الحقيقية).

خصوصية الاتصالات:

سننظر في كيفية امتداد هذا القانون إلى خصوصية الاتصالات.

ان خصوصية الاتصالات:

1. متميزة عن قانون البحث والضبط،
2. أيضا متميزة عن سياسة بيانات المعلومات.

* ملاحظة: التركيز هنا يتعلق بخصوصية الاتصالات ولا يمتد إلى سياسة المعلومات.

وبينما نعمل من خلال تقييم هذا القانون، نأمل ان ترى كيف يتم تطبيق القانون والنظام القضائي باستخدام هذه الأساليب.

حالة أولمستيد (Olmstead) ضد الولايات المتحدة

عملية التعديل الخامس تتقاطع مع خط التعديل الرابع في حالة بويد (Boyd)، حيث أنهى رئيس المحكمة تافت (Taft) النقاش مع قضية جاكسون السابقة. الهواتف لم يكن لها الوضع الدستوري كما كان للبريد في ذلك الوقت. ففي قضية جاكسون، اعتبر البريد من ملكيتك أو من وثائقك حيث من المتوقع أن تكون هذه الملكية البريدية محمية. فالتوقعات ظهرت، لذلك صرح جاكسون بأن هذا الأمر قد تم تغطيته بموجب حقوق التعديل الرابع.

يحمي	التكنولوجيا	جريمة	الاستعارات والرموز	التعديل الرابع
1928 -		التهريب	الممتلكات، التعدي على ممتلكات الغير	نعم
1967-1968	قضية الهاتف- من mass market Title III (1968)	جريمة القمار المنظمة	الناس لا الأماكن - توقع شخصي - توقع موضوعي	محتمل
1984-1986 قانون خصوصية الاتصالات الإلكترونية (ECPA)	البريد الإلكتروني/الاتصالات الإلكترونية. وخدمة التسجيل والبث اللاحق (Forward & Store)	----	بريد من الدرجة الأولى (اقتصادي)	
1994	سجل المعاملات	إرهاب	شك معقول وقابل للتوضيح.	CALEA *

* CALEA: (من المترجم: يفرض هذا القانون الأمريكي على جميع الشركات المزودة لخدمات الاتصالات السلكية واللاسلكية وخدمات إنترنت، أن تقوم بتعديل معداتها، وقدراتها، بحيث يمكن للجهات الحكومية استخدام هذه المعدات لأغراض التصنت والتجسس.)

كان القاضي تافت (Taft) يحاول أن يخلق حجة ويأمل أن تكون وجهة نظر تقدمية حول حدود التعديل الرابع.

المعارضة:

يقول القاضي براندیز (Brandeis) ان هذا الدستور الذي نوسعه ضد هذا القانون.

ما هي حجج براندیز حول الهاتف؟

انه لا يوجد فرق بين الهاتف والرسالة المختومة وبالتالي يستخدم نفس الحالات التي يستشهد بها تافت.

وفي المحكمة الحديثة، فان رأي الأغلبية تحجز الحق في إدراج الرأي المعارض.

كاتز (Katz) ضد الولايات المتحدة

كانت هذه قضية في محيط الجريمة المنظمة.

كان ج. إدغار هوفر (J. dgar Hoover) مدير مكتب التحقيقات الفيدرالي (FBI)، وكان يسجل الكثير من هواتف الناس وكان يعتقد أنه يؤثر على العملية السياسية. ونتيجة لذلك، ومنذ عهد المدير هوفر فان جميع مديري مكتب التحقيقات الفيدرالي كانوا قضاة (باستثناء المدير الحالي –عام 2005–).

متطلب عام لـ "قاضي مستقل ومحايد": للحصول على المذكرة، يجب عليك إثبات سبب محتمل لقاضي منفصل محايد. مهمتهم هي التحقق من مصداقية الحاجة إلى مذكرة.

كتب القاضي بوتر ستيوارت (Potter Stuart) الرأي الاتي: على الرغم من وجود توقع ذاتي للخصوصية، فقد تكون هناك عوامل أخرى تربك هذا التوقع. فيمكن للتوقعات الموضوعية نقض التوقع الذاتي بسبب قوانين المجتمع. فالتوقع الشخصي –كيف يشعرون، التوقع الموضوعي –إلى أي مدى يرغب المجتمع في منح أذونات.

لقد غيرت المحكمة العليا تمامًا الطريقة التي تنظر بها المحاكم إلى التعديل الرابع.

كان رأي بوتر ستيوارت مقبول إلى حدٍ ما، لكن أيضًا تم انتقاده بشدة.

هؤلاء الذين يرتبطون بشخص متوقع قيامه بنشاط إجرامي هم من انتهكت خصوصيتهم، ولذلك كان اتحاد الحريات المدنية يعارض التنصت على الخطوط.

يحدد الباب الثالث (Title III) مجموعة دقيقة من القواعد التي تنتهي في نهاية المطاف بإنشاء مستوى حماية يتجاوز حقوق التعديل الرابع. ويحدد الباب الثالث لوائح استخدام التنصت على المكالمات الهاتفية، والتي تشمل متى لا تعمل أساليب التحقيق الأخرى. ويجب على المسؤولين القضائيين الآخرين الموافقة على التنصت إلى جانب مكتب التحقيقات الفيدرالي. حيث يحدد جزء من الإجراءات وجود فريقين يراجعان مناقشات التنصت. ويتم ذلك في الوقت الفعلي، ويتم وضع ضمانات إجرائية لحماية أولئك الذين لا يستهدفون بالتحقيق.

التعديل الرابع يمكن أن يُعترض من خلال أدلة ممتدة، بمعنى أن الأدلة سوف تختفي أو سيتم قتل شخص ما لذلك يجب التصرف بسرعة.

الباب الثالث (Title III) – متطلبات التخزين/التسجيل ، شرط أنك ستحصل على حساب لما يجري إما قبل أو بعد التنصت، وكان الباب الثالث مخولًا في الأصل لأنواع محددة فقط من الجرائم مثل جريمة المقامرة، والابتزاز المالي.

أصبحت عملية التنصت على المكالمات الهاتفية أرخص ولكن عمليات التنصت ازدادت. ومع ذلك، يبدو أن هناك عددًا قليلاً من طلبات التنصت التي تم رفضها. وكانت الغالبية العظمى من حالات التنصت على المكالمات الهاتفية في التسعينيات تتعلق بالقضايا الجنائية المتعلقة بالمخدرات.

من أجل التنصت على الهاتف، يجب أن يكون هناك أمر محكمة الباب الثالث أو أمر محكمة "قانون مراقبة الاستخبارات الأجنبية" (FISA). وينطبق التعديل الرابع على مواطني الولايات المتحدة وينظم في داخلها.

قانون خصوصية الاتصالات الإلكترونية

بحلول منتصف الثمانينات، أصبحت الخدمات الإلكترونية شائعة. واعتبرت الاتصالات في منتصف الثمانينيات من القرن الماضي وسائل تخزين وبث، وليس اتصالات سلكية. وبدا ان هذا التطبيق على التعديل الرابع مشكوك فيه.

وقد تمت معاملة الاتصالات الإلكترونية والبريد الإلكتروني مثل البريد من الدرجة الأولى (العادي)، وتم إنشاء النظام الأساسي لقانون خصوصية الاتصالات الإلكتروني (ECPA). هذا النظام الأساسي أكثر تعقيدًا من قانون الباب الثالث.

وكانت صناعة التكنولوجيا استباقية خلال هذه العملية، فقد كان هناك اتجاه من عدد صغير من مقدمي الخدمات إلى عدد أكبر بكثير من مقدمي الخدمات.

يومذاك، تم إنشاء قانون خصوصية الاتصالات الإلكتروني (ECPA) لأن الكونجرس اعتقد أنهم كانوا يتبعون أسبقية القاضي براندیز (Brandeis). وينطبق قانون خصوصية الاتصالات الإلكترونية (ECPA) على البريد الوارد في الترانزيت أو البريد الذي لم يستلمه المرسل إليه بعد.

وأصبح الآن إجراء المراقبة الإلكترونية أرخص بكثير من الطريقة التي كانت لأنك تتعامل مع تدفق بيانات إلكتروني. فالتكلفة المنخفضة للتخزين غيرت ديناميكيات الشركات التي تختار الآن الاحتفاظ بالكثير من الاتصالات الإلكترونية (بدلاً من حذفها) وتحديد مكان حفظ البيانات.

وقد تم العمل بقانون خصوصية الاتصالات الإلكتروني (ECPA) لمدة 10 سنوات تقريبا وكان هناك خلاف طفيف حوله خلال ذلك الوقت.

في الأصل، تم ترك الهواتف اللاسلكية غالبًا خارج قانون الباب الثالث وقانون خصوصية الاتصالات الإلكتروني (Title III و ECPA). وقد أغلقت CALEA السابق ذكرها تلك الفجوة وتم عنونة أمرا جديدا في الإنترنت والاتصال الرقمي، ولم يتم حماية سجل المعاملات في كلا القانونين (Title III أو ECPA).

تألفت سجلات المعاملات من ملفات السجل (من وماذا أرسل وإلى من) على عكس المحتوى. وتتكون هذه السجلات من التاريخ والوقت وبعض معلومات الموضوع. وقد خضعت سجلات المعاملات لمتطلبات وصول أكبر من سجلات ذات الرسوم (Toll Records).

قضية تيري ضد أوهايو

(من المترجم: تتلخص القصة في أن شرطي ذو خبرة أوقف 3 أشخاص بعد ان رآهم يتقدمون بالتناوب ذهابًا وإيابًا على طول مسار مماثل، متوقفين للتحديق في نافذة المتجر نفسها لـ 24 مرة).

ان تتابع نظر المتسوقين إلى واجهة متجر قد تعتبر اشتباها. فضابط الشرطة الذي لدية خبرة كافيه (35 سنة) لديه شك معقول منطقي بأن جريمة قد تحدث أو على وشك الحدوث.

هناك إجراء يجب ان يتبع من اجل إنفاذ القانون بالتدخل في حقوق الشخص وخصوصيته تحت بند التعديل الرابع.

أوامر المحكمة التي تستخدم هذه الاستعارة من قضية تيري ضد أوهايو يجب أن تفعل ذلك من طرف واحد.

محاضرة 5: قضايا دولية

المحاضر: مايك فيشر (Mike Fischer)

privacyinternational.org: موقع يقوم بمسوح للحالات التي تعرض وتعلن في المحاكم وهي طريقة مثيرة لتصور الأشياء.

المملكة المتحدة – تم تضييق الخلافات الدولية

لإيجاد بيئة للإنترنت، هناك 4 أدوات فريدة من نوعها:

1. السوق،
2. الترميز (Code) أو المعمارية،
3. القانون،
4. القواعد أو المعايير.

وهنا سنركز على القواعد، حيث:

- في الصين، يحاولون استخدام الترميز (Code) / المعمارية لممارسة السيطرة.
- وتعد سنغافورة واحدة من أكثر الدول تقدمًا من الناحية التكنولوجية في العالم، ولديها البنية التحتية المناسبة لإعداد القوانين واللوائح الملائمة.
- حالة كمبيو سيرف (CompuServe) في ميونيخ:
  – محاكمة لنقل مواد إباحية.
- أكاماي (Akamai)– شبكة من الخوادم المختلفة المنتشرة في جميع أنحاء العالم في مواقع جغرافية مختلفة:
  – وهذا يجعل إزالة المحتوى المسيء إلى بلدان محددة أمرًا يسهل الوصول إليه ويسهل التعرف عليها
- هل يمكنك حجب بعض أجزاء الإنترنت في بلدان معينة؟

هناك ثلاثة عناصر من الحقوق المعنوية: الإسناد (نسبة الشيء إلى صاحبه)، عدم الإسناد أو التأليف الكاذب، منع الآخرين من تعديل أو تدمير أو التدخل في سلامة العمل.

الحقوق الأخلاقية – حقوق غير قابلة للتصرف وتتعامل مع قوانين حقوق الإنسان حالة: في انتظار جودو [2]

الحقوق الثقافية – إمكانية الوصول

– قضية ماوري (Mawry) ضد ليغو (Lego)

– التوافق يضمن أن ليغو يفوز في هذه الأنواع من الحالات. وأيضا اتفاقيات التجارة الحرة.

في هذه الفئة، يمكن التفكير في النظام القانوني من حيث الرسم البياني فن Venn (من المترجم: التعبير عن العلاقات بين الأشياء برموز منطقية نستخدم الدوائر).

[2] من المترجم: "في انتظار غودو Waiting for Godot"هي مسرحية لصموئيل بيكيت (Samuel Beckett)، استوحاها من لوحة لكاسبار ديفيد فريدريخ لرجلين ينظران إلى القمر وينتظرون "غودو" .. حيث أن "غودو" هو الغائب (أو ربما الشيء) الذي ينتظره الجميع ولا يأتي..

# # # # # # #

لقطات لأجزاء مختلفة من العالم للنظر في صراعاتهم حول المشاعات الرقمية والإنترنت:

(محاضرين زائرين)

عرض: أنيتا تشان (Anita Chan)

أمريكا اللاتينية: تطوير البرمجيات الحرة في بلدان أمريكا اللاتينية. أيضا الصراع حول المواطنة والمجتمع تتطلب من هذه البلدان توفير أو تفويض استخدام البرمجيات الحرة من الإدارة.

الأسباب الحكومية التي تدعو إلى تطبيق البرمجيات الحرة:

- البرمجيات الحرة لديها حوافز مالية – هي أرخص وأكثر استدامة في بلدان أمريكا اللاتينية،
- يمكنها ان تقتصر على مزود خدمة واحد،
- لم تعد التكاليف باهظة،
- تعزيز محو الأمية الرقمية،
- إمكانية تقوية الصناعة المحلية.

تشير الحالات أن المستهلك لديه الحق في الوصول إلى المعلومات والخصوصية. وقد تحدث الفضائح حول عمليات تزوير التصويت على أساس شبه منظم (من المترجم: كون البرمجيات الحرة يمكن تعديلها). وفي العديد من هذه البلدان، هناك برمجيات حرة قيد الاستخدام، ولكن السؤال الحقيقي: من يستطيع الوصول إلى هذه الأدوات، وكيفية تشريعها.

برامج التدريب الحكومية أيضا لها علاقة بالتدريب. يمكن تتبع حركات البرمجيات الحرة كارتفاع للسياسة الليبرالية. ويرى مبرمجو البرمجيات الحرة أنفسهم على أنهم جزء من رقمنة العالم.

نأمل أن يتم مشاركة تطوير البرمجيات عبر المؤسسات.

تم إطلاق مشروع PC المستمر. والكثير من التطوير يتم داخل الجامعات البرازيلية.

هناك الكثير من الهيئات التي تعمل حول تطوير البرمجيات الحرة، لكن المواطنين الذين هم مستخدمي البرمجيات الحرة والمطورين هم الأكثر أهمية في دفع هذا إلى الأمام.

حقوق السيادة – المساءلة من قبل المواطنين والوصول إلى التدريب (المثال البرازيلي).

# # # # # # #

كيلتي (Kelty) وثقافة قارب البنط [3]– ما هي المعايير بين الثقافة والشرعية؟

ما هي رخص المشاع الإبداعي (Creative Common)؟ هناك مستويات مختلفة من التراخيص التي يمكنك اختيار ربطها بعملك أو ملكيتك. هناك حوالي 12 أسلوب متنوع.

{رخص المشاع الإبداعي: رخص تسمح بنسخ ونقل ومشاركة وترجمة
وأحيانا تعديل الملفات التعليمية أو التدريبية وخلافها – المترجم }.

من أين تأتي أفكار التراخيص المختلفة؟ يصف براون (Brown) نتيجة التراخيص هذه كنتيجة لمناقشات مع مجموعات مختلفة تحدث معها. يجادل هو وكريس كيلتي (Chris Kelty) بأنهما "يفعلان الثقافة" فيما يتعلق بحقوق النشر. هذا أمر قابل للإنفاذ إلى حد ما.

عرض:

<u>الهند</u>

مشاركة المصدر المفتوح على البرمجيات الاحتكارية:

هناك فكرة عن مساحة متوسطة بين الممتلكات التجارية والممتلكات الحكومية. وهذا التقسيم يشكل المجتمع المدني.

التركيز على التقسيم الهيكلي وكيفية تأثير ممارسات المعمارية والبرمجيات على مدينة بومباي.

(الأدوات التفاعلية للموارد المجمعة CRIT)؟

صناعة البرمجيات – هناك مجموعة صغيرة من النخبة لديها البرمجيات، والبقية يصبحون قراصنة لأن الآخرين يغالون في السعر، وهذا هو أيضا مماثل في العمارة (المعدات) كذلك. ولا يملك المواطنون هذه المعلومات، لذا ينتهي بهم المطاف إلى دفع ثمنها.

القوانين في الهند أكثر مسامية (ذات ثقوب) وغير جدية. ومنهجية تنفيذ القرار من أعلى إلى أسفل لا تعمل في الهند، وهذا هو ما كان عليه الاستقلال. هذا هو أيضا الفرق في الهندسة المعمارية بين الصين والهند: منهجية من أعلى لأسفل مقارنة بمنهجية من أسفل إلى أعلى.

# # # # # # #

[3] من المترجم: البنط (Punt) هو زورق طويل وضيق ذي قاع مسطح ومربع عند طرفيه ويدفع بعمود طويل، يستخدم في المياه الداخلية أساسًا للاستجمام.

عرض الضيف:

إيران:

لقد مرت إيران بسلسلة من الأفعال الثورية لإيصال الحكومة إلى الدبلوماسية. في أواخر سبعينيات القرن العشرين، كانت هناك ثورات ضد اغتصاب الملكية التي استحوذت على حقوق المواطن.

لا تزال سياسات إيران عالقة في هيكل مزدوج للسلطة. منذ الثورة، وحتى البرلمان السابع الآن. والقرآن لا يستخدم لاشتقاق البنية القانونية للمجتمع الإيراني، فهناك صراع مقسم بين النداءات إلى دين إسلامي وبين الآراء التاريخية للدستور.

الحكومة تقوم بالأشياء خارج القانون. هناك فترات يتم فيها إغلاق الصحف الدورية.

القانون السيبراني والقرصنة (Cyberlaws and Hacking)

هناك حاجة إلى قوانين تنظيمية بشأن القرصنة والمحتوى على الإنترنت (المواد الإباحية، إلخ.)

هناك 3 مشاريع قوانين قيد التداول في البرلمان الإيراني حيث يجب أن تكون جميع المداولات علنية.

1. فاتورة الجريمة السيبرانية – قدمت إلى البرلمان قبل شهرين، ولكن لم تتم مناقشتها:
   - يتعامل مع القرصنة، والوصول إلى المعلومات المصنفة، وفروق العمر لتوفير محتوى غير مناسب لمجموعات معينة (مثل الصغار)؛ والتشهير وسمات الشخص غير الموثوق.
2. حرية المعلومات – ترويج قوي لشؤون نائب الرئيس:
   - فكرة لتعزيز الديمقراطية والشفافية؛ يمكن للمواطنين الوصول إلى المعلومات مع استجوابهم وحرية انتقاد سلوك الحكومة مع عقوبة.
3. حماية الخصوصية – مراقبة:
   - لكل نوع من التحقيق والحجز. فان التنصت على المكالمات والتتبع يعتبر غير قانوني بدون مذكرة قانونية.

أن إيران تدعم أيضًا برمجياتها لتصفية (تنقية) المواد.

المحاضرة 6: التحولات الحدودية العامة والخاصة القائمة على التكنولوجيا

المحاضر: هال أبلسون (Hal Abelson)

التشفير

مراجعة كيفية عمل تقنية التشفير. سنناقش الفترة من 1980 إلى 2001 التي تم التحول فعليا من التكنولوجيا العسكرية والأسلحة إلى الاستخدام اليومي المألوف. التفكير جديا في التشفير كضغوط سياسية ترتبط بإدخال التكنولوجيا الجديدة.

مطبات التكنولوجيا والسياسة

- كلمة "خصوصية" لها ارتباطات معينة تقوم بها، ولا يوجد أي منها له ارتباط فعلي بالإنترنت.

– منذ حوالي 10 سنوات، كلمة "البريد الإلكتروني" لم يكن لها معنى حقيقي لأن لا أحد استخدمها فعليا.
– صورة الثقة في مشغل البريد هي ليست ذات الثقة عندما نتكلم عن البريد الإلكتروني أو التشفير.

السرية (Confidentiality): ان تهتم بان المستلم المقصود فقط هو من يستلم مصادقة الرسالة.
النزاهة (Integrity): كيف تعرف انه لم يعترض أحدا الرسالة، وعدم التنصل من استلام الرسالة (لا تستطيع لاحقا النفي بانك استلمت الرسالة).

هذا استعراض لمن تعامل بالتشفير، ويشار إليها بالتواقيع الرقمية:

1. تشفير ما قبل التاريخ (قبل 1970)،
2. تشفير المفتاح العام،
3. سياسة التشفير.

تشفير 1900 قبل الميلاد:

يعتقد انه من أقدم أشكال التشفير التي عرفها الإنسان هي ما يطلق عليه الهيروغليفية.

كان جيفري شوسر (Geoffrey Chaucer) شاعراً وفلكياً. كما كتب أول دليل علمي بالإنجليزية في دراسة على الإسطرلاب. (وفي جزء من هذا الكتاب، استخدم التشفير. –تمرين الصف–). استخدم شوسر تنسيقًا يسمى التشفير البديل. بحيث يحدث الاستبدال البسيط أو الأحادي عندما تستبدل دائمًا بنفس الطريقة.

واستخدم يوليوس قيصر تشفير الاستبدال حيث تقوم بتحريك كل حرف بنفس الطول ليحل محلها.

في القرن التاسع، كتب يعقوب (Yaqub) كتابًا يعرف الآن باسم تحليل التكرار. (رسم بياني لمتوسط تكرار الحروف باللغة الإنجليزية.)

هذه هي التقنية (التشفير) منذ القرن التاسع.

بعد مرور ألف عام، ما زال هذا النوع من التشفير قيد الاستخدام. ما زال الناس يستخدمون أساليب غير آمنة في التشفير. فلو ذهبت على الإنترنت قبل خمس سنوات من الأن، لوجدنا بعض الشركات لا تزال تقوم بتسويق منتجاتها بطريقة غير آمنة أو بطريقة تشفير سيئة.

*** تشفير فيجينير(Vigenere):**

فيجينير نشر وعمم هذا النوع من التشفير، ولكن في الواقع ان البيرتي (Alberti) هو من قام بإنشائه. فالحروف الزرقاء هي المفتاح. الحرف "a" يذهب إلى "S"، ثم ينتقل الحرف "b" إلى"O" وتقوم بدورة على الحروف من خلال استبدال كل حرف. ويعتبر ذلك طفرة كبيرة في التشفير منذ 500 سنة، وكان يعتبر نظام للتشفير غير القابل للكسر. ولكن في الواقع، تم كسره في منتصف القرن التاسع عشر.

*** كسر تشفير فيجينير:**

تم تحويل التشفير إلى مسائل توزيع التكرار المختلفة بسبب ان اللغة الإنجليزية لها طول طبيعي. والجزء الصعب هو العثور على طول المفتاح. وفي نهاية عقد عشرينيات القرن العشرين (1920's)، معظم البلدان كان لديها أجهزة تشويش سوداء (Black-Jammers) وهي عباره عن غرف للرياضيات لتكسير التشفير.

اخترع فريدمان (Friedman) فهرس الصدفة لكسر التشفير. لم يكن أحد يعرف أن باباج (Babbage) قام بالفعل بكسر كود فيجينير حتى عام 1920 حيث انه لم يعلن كسر التشفير.

كثير من الأشخاص الذين يقومون بهذا العمل لا يحصلون على الشهرة في هذا المجال لان أعمالهم تنتهي بان تصنف سرية لا يطلع عليها الجمهور.

المفتاح يكون بطول الرسالة:

التشفير الآمن المؤكد هو لوحة المرة الواحدة (one-time pad)، بحيث يجب اختيار المفتاح بشكل عشوائي ويتم استخدامه لمره واحدة فقط. ولكن يجري العمل حاليا للعثور على شيء أكثر أمنا. ونشأ مشروع فينونا (Venona) في عام 1943، وظهرت فيه الكثير من الأمثلة على تشفير اللوحة لمرة واحدة. كلود شانون (Claude Shannon) – بطل نظرية المعلومات.

اخترع شانون كلمة "بت" (bit). وقدم شانون لأول مره تعريف رسمي لما يعنيه أن تكون آمنًا، أو تشفيرًا. (نتائج بحث "السرية التامة"Perfect Secrecy لشانون 1949).

الأشياء المصنفة (السرية) الحقيقية الآن هي الطرق والأساليب لإنشاء لوحات عشوائية. من الصعب فعلاً عمل منصات جيدة لمرة واحدة. يوجد حاليا تشفير متدفق وهو تشفير البت الثماثلي لفيجيتير.

DES (معيار تشفير البيانات) أصبح الآن قديم حيث قامت وكالة الآمن القومي الأمريكي (NSA) بتعديل الخوارزمية لجعلها أكثر أمانًا. بالنسبة إلى DES فيمكنك تقسيم الرسالة إلى مجموعات من 64-بت ثم القيام بتحويل S-box (استنادًا إلى مفتاح 56 بت) ثم إعادة وضعه سابقا. هذا فعال إلى حد ما لأنه مجرد مزج ويمكن فك شفرته بسهولة. طريقه منضبطة في التشفير ومن السهل إرجاعها إلى أصلها.

أمن DES: الطريقة الوحيدة لكسر شيفرة DES هي في الأساس باستخدام هجوم التخمين (Brute Force). يعني جرب جميع المفاتيح! في عام 1965، كان 2 ^ 56 عددًا كبيرًا جدًا من المفاتيح. ولكن الأن ليس كثيرا. وقد كانت الحكومة ضغطت على الناس لعدم استخدام أي شيء غير DES (المعهد الوطني للمعايير والتكنولوجيا–NIST).

مبدأ كيرخوف (Kerkhoffs):

قام بأعداده اللغوي البلجيكي الذي كتب دليلًا حول الخصائص الجيدة لأنظمة التشفير. وأحد المبادئ هو تصميم النظام بحيث يكون هناك جزء صغير من المعلومات التي تحتاج إلى تأمين، وبالتالي يكون أفضل تصميم. والأمان يجب ان يكون في اختيار المفتاح وليس في ميزات التصميم الغامضة.

اندرو "Bunnie" هوانغ – كسر التشفير على XBox. وقانون حقوق الملكية في الألفية الرقمية يمنع الأشخاص من نشر أو توزيع المعلومات المحمية بقانون حقوق النشر.

ومبادئ التشفير المبكرة لا تعمل بشكل جيدا في عصر الإنترنت.

فكرة رائعة: يمكن إنشاء مفتاح مشترك مع أشخاص لم يلتقوا أو لم يتصلوا من قبل ولم يتخذوا أي ترتيبات مسبقة.

نظم التشفير (Cryptosystems)

أنواع مختلفة من الهجمات:
اختيار نص صريح: 300 من نفس الحرف.
خرطوم مطاطي – للفوز على الناس بالخرطوم المطاطي ... (من المترجم: خرطوم مطاطي Rubber Hose تعني تحصيل كلمات السر أو مفتاح التشفير من المستعمل بالقوة).
وليس منها ما هو مناسب لتطبيقات الإنترنت لأنه يجب التلاقي لأجل تبادل المفتاح.

ديفي (Diffie) كان طالب دراسات عليا في معهد ماساتشوستس للتكنولوجيا حيث التقى مع مارتي هيلمان (Marty Hellman)، الذي كان يعمل في ستانفورد. في حين ان رالف ميركل (Ralph Merkle) كان طالباً في جامعة بيركلي. يعتقد بان ميركل هو الشخص الذي كان وراء فكرة تشفير المفتاح العام (Public–Key Encryption)، لكن هيلمان وديفي كتبا الخوارزمية حيث قاما بنشر ورقة الاختراق المطلقة (Absolute Break–Through) في عام 1976.

منذ حوالي 8 سنوات فقط، تم اكتشاف أن كليفورد كوكس (Clifford Cocks) ومالكولم ويليامسون (Malcolm Williamson) قاما في عام 1973–1974 بعمل سري في مجال التشفير في الاستخبارات البريطانية.

الفكرة الأساسية لـ ديفي–هيلمان–ميركل:

الفكرة: كيف يمكنك تبادل المعلومات السرية حتى إذا كان شخص يسمع ما تقوله للآخرين؟

أليس تحسب رقمًا استنادًا إلى معلومات سرية حول ما تعرفه فقط
بوب يحسب رقمًا استنادًا إلى معلومات سرية حول ما يعرفه فقط
في النهاية، سيكون هناك رقم سري يعرفه فقط أليس وبوب.

النهج العام هو استخدام تشفير أحادي الاتجاه.

على احدى وجهي العملة، مشكلة يمكنك القيام بها باستخدام آلة حاسبة صغيرة وعلى الوجه الآخر، يوجد مشكلة حسابية مكثفة. وبناءا على قانون الأس، سيكون بوسع كل من بوب وأليس الحصول على نفس الرقم حيث يستطيعوا استخدامه كمفتاح مشترك لتواصل التشفير. لأي تنصت، يتطلب حل مشكلة السجل المنفصل (سريع).

التوقيع إلكتروني: من الممكن لك إنتاج توقيع والذي يمكن لأي شخص فحصة أو التأكد منه، ولكن من الصعب إنتاج المصداقية وعدم التنصل.

الشهادات والهيئات التي تصدر الشهادات: ستحصل أخيرًا على سلسلة لسلطة تصدر الشهادات وتكون معروفة جيدًا لتؤكد المصادقة.

بروتوكول أمن طبقة النقل الأساسية الذي يُعرف باسم (SSL): في هذه الحالة، هناك شهادة عميل يؤكد أنك أنت الشخص الذي عرفت على نفسك.

لم ينتج ديفي وهيلمان طريقة عملية لتشفير المفتاح العام. وفي وقت لاحق تم إنتاج خوارزمية RSA والتي يمكن استخدامها لكل من المفتاح العام والتوقيع الإلكتروني وقد سعى كل من معهد ماساتشوستس للتكنولوجيا وستانفورد للحصول على براءات الاختراع. وقد كانت RSA براءة اختراع جيدة، لكن المفتاح العام كان براءة اختراع ضعيفة. وقد شكّل معهد ماساتشوستس للتكنولوجيا (MIT) مع ستانفورد شراكة المفتاح الرئيسي وشكلوا اتحاد لاحتكار المنتج وقد رفضوا ترخيص استخدام المفتاح العام للآخرين ما لم يستخدموا أيضا براءة اختراع RSA. وبقي المفتاح العام مغلقا حتى عام 2001. وفي الوقت الحاضر يوجد العديد من المفاتيح العامة المشفرة المنتشرة.

في نهاية العام 1970 كان بوبي ري (Bobby Ray) رئيسا لوكالة الآمن القومي الأمريكية عصبيا للغاية. فقد كان التشفير وما يزال سلاحا عسكريا وقد بدأت وكالة الآمن القومي الأمريكي (NSA) بالتحدث عن التشفير علنا. وقد كان هناك اجتماع بين معهد ماساتشوستس للتكنولوجيا ووكالة الآمن القومي الأمريكي، وكان معهد ماساتشوستس للتكنولوجيا مترددًا بشأن بقاء أي عمل داخل الحرم الجامعي سريا. وكإجراء مجاملة، تم الاتفاق على ان يرسل المعهد الأبحاث والمعلومات إلى وكالة الأمن القومي وإلى الوكالات الأخرى كما يرسلها إلى الزملاء.

جعل لويس فريه (Louis Freeh) هذا الأمر أولوية قصوى في مكتب التحقيقات الفيدرالي. وفي عام 1994، كان التشفير شكلاً من أشكال التكنولوجيا الغريبة لأنه كان يُخشى من أن يستخدم في الإجرام والإرهاب.

كليبر (Clipper)

الجمهور لا يرغب باستخدام الهواتف المشفرة، حيث تم تصميم رقاقة كليبر (Clipper) بواسطة وكالة الأمن القومي وهي تسمح للأفراد بإجراء مكالمات مشفره مع باب خلفي. وعليه ... فما رأيك في هاتف كليبر هذا؟ شركات صناعة الهاتف رفضته. الشرائح المحصنة ضد العبث من شأنها أن ترفع التكاليف.

حروب مؤتمن المفتاح (Key Escrow)

- تألفت من سياسة حرب معقده ذهابا وإيابا.
- كانت الوكالات تسعى للحصول على اعتماد أجندتها من مجلس الكونغرس والجواب هو التحكم بالتصدير.

إذا كنت تعمل في بيع برمجيات ومنتجات التشفير، فسيتم تسجيلك كتاجر أسلحة. قبل عام 1995، تم تصنيف تكنولوجيا التشفير من قبل وزارة الخارجية كذخيرة.

تم استبعاد مجموعة من الدول من استخدام تكنولوجيا التشفير وهي: سوريا، السودان، وليبيا.

كانت هناك شائعات في عام 1995 أن مجلس الأمن القومي الأمريكي لديه مشروع التنصت على جميع مشاريع الاتصالات التي كانت قيد التنفيذ، ويعتبر هذا المشروع سري ولم يتحدث عنه أحد ولا عن ماذا يحدث بالضبط في عملية التصنت.

اما مشروع Echelon فقد كان يتنصت على الكثير من الاتصالات حول العالم.

في النهاية انهارت جميع محادثات ونقاشات المعهد الوطني للمعايير والتقنية. ان بناء هذه الأنظمة يعتبر رخيصا للغاية ولكن المستهلكين لا يدركون ذلك.

مايو 1996

حسناً، يا رفاق يمكن أن يكون لديك تشفير ولكن عليك أن تسجل مفتاحك مع مؤتمن هذا المفتاح. سوف نقوم بتزاوج الأفكار فيما يتعلق بالتشفير والتجارة الإلكترونية. فالبيت الأبيض اعتبر ان سعر الشهادة والسماح بالتجارة الإلكترونية يعتمد على تأمين (ضمان) المفتاح.

التشريع 1997

كانت هناك عقوبة في حال بناء الإلكترونيات دون مفتاح الائتمان (Escrow Key) وكان هناك أيضا مشروع قانون يحظر على الكونغرس التخلص من تصدير المنتجات. وفي الورقة البحثية "مخاطر استرداد المفتاح، ..."، تقرر أنه لن يكون هناك نقاش حول الحريات المدنية. هدفت هذه الورقة لمعالجة مخاطر وقف الجريمة ثم التحقيق في التحليل الفني لوجهات نظرهم.

ملاحظات فنية:
من يستطيع الحصول على مفاتيح الائتمان أيضا والتي يستطيع مسؤولي الحكومة الوصول إليها بسرعة.

حوالي عام 2000، تم تحرير قوانين التشفير. ففي عام 1994، لكل فرد أو مؤسسه تستخدم برمجية يجب ان يتوفر لديهم رخصة تشفير. هذا هو نتيجة ان التجارة الإلكترونية تجاوزت الصناعة.

ثم جاء في سبتمبر 2001...
السيناتور جود جريج (Judd Gregg) وقف أمام الكونجرس الأمريكي وقال: يجب علينا ان نفعل شينا بخصوص التشفير. يعتبر ذلك أساسا في بناء التشريع والذي تم في تشريع 1997. انتهت الجهود وذلك بسبب عدم موافقة الأعضاء على دعم التشريع. وفي شهر أكتوبر، تراجع السيناتور جريج عن تقديم التشريع.

ما الذي تغير؟

في عام 1995، كان الارتباط بين التشفير والبريد الإلكتروني شيء مختلف. ولكن التشفير الأن يعني حماية بطاقاتك الائتمانية وو...الخ، مما حول التشفير إلى أمور استهلاكية. انها معاني الكلمات التي شكلت الآن التكنولوجيا والسياسة اليوم. والذي لم ولن ينتهي.

الآن علينا إجراء تعديل آخر حول الأمان في الهاتف. أي نوع من سلطة التنصت يجب ان تمتلكها الحكومية؟ ماذا عن تطبيقات الإنترنت مثل سكايب؟ هل يجب عليك الالتزام بلوائح CALEA؟

على مدار العامين المقبلين، سنشهد المزيد من التغييرات وربما قوانين حول التطبيقات على الإنترنت.

محاضرة 7: التنميط والتنقيب في البيانات (Profiling and Datamining)

المحاضر: داني فايتسنر (Danny Weitzner)

السيارات والطائرات:

التنميط والتنقيب في البيانات بعد 9/11

مناقشة: لوجستيات الامتحان النصفي

التمييز بين وقائع القضية وكيف ينطبق القانون على الوقائع. يجب الحفاظ على الحقائق والقانون منفصلين عن بعض.

مناقشة – ورقة نهاية الفصل والجدول الزمني.

السيارات:

لقد انتقلنا إلى حد بعيد من حيث كنا في إنجلترا إلى يومنا هذا في الولايات المتحدة حتى نمتلك فهمًا أوضح عن وقت حدوث أي تعديل في التعديل الرابع (4th amendment).

ما نراه في تطور التعديل الرابع، انه في وقتنا الحاضر لم يعد هناك حدود واضحة عندما تتجاوز الحكومة الخطوط. ولقد قضت المحكمة الكثير من الوقت في محاولة لإعادة بناء هذه الخطوط. وأصبح العالم الآن أكثر تعقيدًا بكثير حيث أصبح الناس يستخدموا وسائل أخرى (الطائرات والسيارات) ويستخدمون التكنولوجيا للقيام بالجرائم الأخرى، لكن هناك أيضًا نقاط مهمه تجعل مهمة فرض القانون أكثر سهولة.

السيارات – فالسيارات تزيد من قوة وقدرة الناس على القيام بالجريمة والهروب بشكل أسرع. لقد تم الأخذ بعين الاعتبار العديد من التعديلات على التعديل الرابع فيما يتعلق بـ متى وكيف يستخدم الناس للسيارة.

مدينة انديانابوليس مقابل مدينة ادموند (Indianapolis vs. Edmond):

كيف يتم العمل؟ الإيقاف والتفتيش القياسي: ان جهة إنفاذ القانون تعمل على إيقاف كل كذا (عددا ما) من السيارات على نقط التفتيش. ويقوم الموظف بالبحث البصري الخارجي في السيارة. وتستخدم الكلاب للشم حول السيارة.

الفكرة هنا ان إيقاف الشرطي لسيارتك لفترة قصيره من الزمن يعتبر تعدي واستيلاء على الممتلكات الشخصية في الوقت الحالي.

التعديل الرابع (4A):

- تفتيش / مصادرة،
- إذن،
- معقولية،
- الاشتباه:
  - الاحتياجات الخاصة والترابط "الفوري"،
  - المعايير (لا يمكن إيقاف السيارات العشوائية بناء على الشك).

القاضي أوكونر (O'Conner) جعل من القضية أنها بحث معقول وأن عددًا كبيرًا من السيارات تتوقف. وان هذا ليس عشوائيا. بالإضافة إلى ذلك، لا يوجد سبب للاعتقاد بأن السيارات التي توقفت مشبوهة. ويقول رئيس القضاة راينكويست (Rheinquist) في معارضته أنه يجب أن يكون هناك نوع من التوازن، لكن القاضي أوكونر لم يوافق.
يعتقد القاضي أوكونر أنه يجب أن تكون هناك أمور خاصة يجب أن تحدث من أجل إجراء بحث معقول كهذا. ولكن أوكونر يريد الذهاب إلى اتجاه تضيق في التشريعات لفحص هذه الأمور والاحتياجات الخاصة ومن الأمثلة عليها هي اختبار المخدرات، والقيادة في حالة سكر. واستنادًا إلى معيار عدم إيقاف السيارات العشوائية بناءا على الشك، يحاول القاضي أوكونر حماية الحقوق الشخصية.

وقد أدركت المحاكم أنهم لا يعرفون ما يحدث بالضبط في ذهن الضابط الذي يوقف السيارة. والشيء الرئيسي حول نقاط التفتيش المعتدلة هو أنه إذا وجدت شخصًا يقود سيارته وهو مخمورا على الطريق يجب ان يخرج من الطريق لأنه يشكل خطر على السلامة العامة. لكن استخدام نفس المنطق في المحاكم لشخص يتناول المخدرات ويقود سيارته لم يكن كافيا للمحاكم.

بعد فترة وجيزة من البت في هذه القضية، حدثت أحداث الحادي عشر من سبتمبر وتم إقرار قانون باتريوت (Patriot). وهذا القانون (باتريوت): وسع حقوق إنفاذ القانون للحصول على المزيد من المعلومات عن المتطرفين في داخل وخارج الولايات المتحدة الأمريكية.

وخطابات الأمن القومي: تعادل أمر الاستدعاء ولكنها لا تأتي من المحكمة. بدلا من ذلك هي تأتي من محكمة مراقبة الاستخبارات الأجنبية (محكمة سرية للمخابرات الأجنبية). ويمكن للمحاكم تطبيق المعايير التي حددها "قانون مراقبة الاستخبارات الأجنبية" (FISA) في المحكمة.

ما هي معايير محكمة FISA؟
ما قبل قانون باتريوت (Pre-patriot)- وكلاء قوة أجنبية
ما بعد قانون باتريوت (Post-patriot) – امتد الأمر لتغطية النشاط الإرهابي المحلي.

هل تستطيع محكمة FISA التنصت على هواتف اثنين من المواطنين الأمريكيين الإرهابيين؟ نعم، يمتد قانون ما بعد باتريوت إلى الإرهاب المحلي.

تغييرات أخرى في قانون باتريوت، شملت:
- قاض واحد داخل 20 ميلا من العاصمة،
- التسلل واختلاس النظر بالمعنى الواسع،
- فحص التسلل واختلاس النظر: بناء ان معرفة متقدمة بان شيئا سيحدث.
- أصبح التنصت السلكي والمتنقل أكثر سهولة في الاستخدام: حيث يسمح بالتنصت على شخص في المحيط الجغرافي.

الدائرة التي عارضت قانون باتريوت -وكان مستغربا- هم أمناء المكتبات بسبب السجلات التجارية، ومثل ذلك تطبيق الإخطار المؤجل على السجلات التجارية في المكتبات كذلك.

قبل قانون باتريوت، كان هناك جدار بين سياق المخابرات الأجنبية والتحقيق الجنائي. في أعقاب 11/9 مباشرة، اعتبر هذا الجدار مسؤولاً عن فشل الاستجابة لمكتب التحقيقات الفيدرالي، ونتيجة لذلك، تم تخفيض الجدار بشكل كبير.

قبل قانون باتريوت، كان هناك جدار فصل بين سياق المخابرات الأجنبية والتحقيق الجنائي، ولكن في أعقاب 911 مباشرة. اعتبر هذا الجدار مسؤولاً عن فشل مكتب التحقيقات الفيدرالي في الاستجابة. نتيجة لذلك، تم تخفيض هذا الجدار بشكل كبير.

الاستخبارات الأجنبية، والتحقيق الجنائي:

كان هناك قلق من أن القضاء على الجدار سيؤدي إلى انتهاك حقوق التعديل الرابع. وتريد اللجنة (لجنة 11/9) تشجيع المشاركة عبر الخط، لكنها تريد التأكد من أن الحقوق الفردية محمية ولا يتم إساءة استخدامها.

انطلاق الحدث: نقل المعلومات الواردة إلى خارج نطاق سلطة قاض معين.

ونتيجة للإرهاب تم القضاء على الجدار بسبب طبيعته، فالإرهاب لا يحدث في أي منطقة.

الاستخبارات الأجنبية، المركز الوطني لمكافحة الإرهاب – NCTC (مسؤولة عن الجدار):

- وكالة الاستخبارات المركزية (CIA)،
- وكالة الآمن القومي الأمريكي (NSA)،
- وكالة الاستخبارات الدفاعية (DIA)،
- الوكالة الوطنية الأمريكية للاستخبارات الجغرافية المكانية (NGA).

التحقيق الجنائي:
- مكتب التحقيقات الفدرالي (FBI)،
- إدارة مكافحة المخدرات (DEA)،
- وزارة الأمن الداخلي (DHS).

أحداث الحادي عشر من سبتمبر أعادت ترتيب مجتمع الاستخبارات الوطنية، وأصبح للوكالات مسؤوليات مختلفة عما كانت عليه من قبل. ومن خلال التحقيق الذي أجرته اللجنة، فإن التنسيق الذي يجب أن يحدث لمشاركة المعلومات وتحديد التهديدات لم يتحقق حتى الآن.

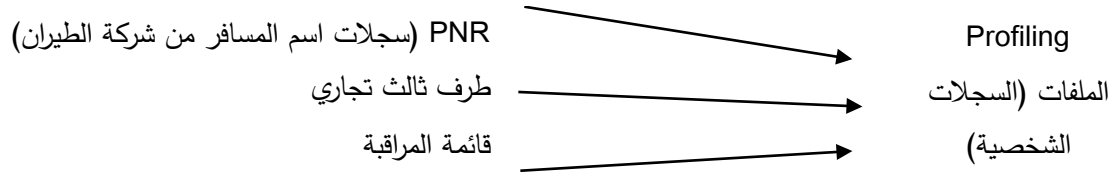
جزء واحد من استراتيجية الأمن الداخلي الرئيسية التي نتجت منذ أحداث سبتمبر هو التحول من التحقيق إلى الوقاية، لذا فإن المهمة الكبرى لمجتمع إنفاذ القانون هي معرفة من هم هؤلاء الأشخاص، ومنع حدوث الجريمة.

طائرات:

منذ 11 سبتمبر

أول شيء نريد منعه هو وصول الأشرار إلى الطائرات. والآن تم تخطي إنشاء وزارة الأمن الداخلي ...

نحن الآن جزء مهم من الحكومة الأمريكية المسؤولة عن اتخاذ القرارات بشأن من يمكنه الركوب على طائرة أو من يمكن تفتيشه. يفعلون ذلك عن طريق الملفات (السجلات الشخصية Profiling).



كابس 2 (CAPPS II) –

من المترجم { CAPPS II ويعني النظام الثاني لفحص الركاب بمساعدة الحاسوب (The Computer Assisted Passenger Prescreening System II) هو برنامج تابع لوزارة الأمن الداخلي بالولايات المتحدة (DHS) تم إنشاؤه لزيادة الأمن في المطارات من خلال تقييم مستوى مخاطر الركاب قبل السماح لهم بالصعود، وهذا البرنامج يبحث لفي المعلومات المخزنة في قواعد البيانات الحكومية والتجارية ويخصص مستوى من المخاطر المرمزة بالألوان لكل مسافر، وفي خضم الجدل من منظمات مثل الاتحاد الأمريكي للحريات المدنية(ACLU) ، ومركز معلومات الخصوصية الإلكترونية (EPIC)، ومؤسسة الحدود الإلكترونية (EFF) ، تم إنهاء هذا البرنامج من قبل الرئيس بوش في أغسطس 2004، ثم تم استبدال البرنامج بـ برنامج مماثل يسمى الرحلة الآمنة (Secure Flight) في أوائل عام 2005}.

يتم نشر السجلات الشخصية في السجل الاتحادي. ويتضمن ذلك خطوتان:

- المصادقة،
- تقييم الخطورة: وضع الأفراد في تصنيفات من خلال فحص قوائم المراقبين.
- المطابقة.

الإجراء الروتيني: اعتقال/ مذكّرة تفتيش.

لأي غرض يتم استخدام هذه السجلات؟ أحد الاستخدامات الروتينية هو إتاحة المعلومات للوكالات التي يكون فيها الأشخاص قد ارتكبوا جرائم بارزة، بالإضافة إلى المحافظة على سلامة الركاب.

لم يتم تنفيذ كابس 2 ولم يتم تشغيله.

الرحلة الآمنة

من المترجم {بناء على ان الحكومة الأمريكية ستتولى مسئولية شركات الطيران في التحقق من أسماء الركاب ضد قوائم مراقبة الإرهاب، تم استحداث نظام جديد سمي "الطيران الآمن" (Secure Flight) لأجل التحقق من هويات المسافرين المحليين من خلال مقارنة معلومات المسافرين المقدمة إلى شركات الطيران في قواعد البيانات الحكومية، والهدف هو تقليل عدد الأشخاص الذين تم اختيارهم لإجراء فحص إضافي في المطارات واستهداف أولئك الذين يحتاجون إلى فحوصات إضافية دقيقة. ولن يسعى النظام الجديد إلى التعرف على أي شخص آخر غير الإرهابيين المعروفين أو المشتبه بهم}.

تحت هذا النظام، فإن الجمهور لديه فرصة للتعليق على اقتراح نظام السجلات.

فما الذي تغير بين كابس 2 والرحلة الآمنة؟

كانت "الرحلة الآمنة" اقتراحًا لاختبار النظام. فقد كانوا يقومون بالاختبار استنادًا على بيانات شهرا واحدا. وشركات الطيران لديها البيانات منذ يونيو 2004. وإشعارات نظام السجلات تم نشره في سبتمبر 2004، وتم إجراء الاختبار في مارس 2005. وبعد جمع البيانات تم إشعار الجمهور.

عندما وصل الأمر إلى أمن الرحلات قاموا بإزالة استخدام الاعتقالات ومذكرات الاعتقال.

شفافية الإجراءات – هذه العملية برمتها تبرر القوانين التي كانت قائمة منذ عام 1974، فقد كانت عملية التطوير مرتبطة بنوع ما من الشفافية. ان الوكالة الحكومية المعينة كانت صريحة حول أخطاؤهم والإجراءات التي يتم تنفيذها.

الآن دعونا نركز على الملفات المختلفة التي حصلت في استعلامات قاعدة البيانات. هل هناك أي انتهاك على التعديل الرابع في عملية الاستعلام هذه؟

ما هو البحث الذي يحدث عندما يتم الاستعلام في حزمة من قواعد البيانات التي تحتوي على معلوماتك الشخصية؟ إنه بحث مشكوك فيه، فكل من يسافر بالطائرة يمر عبر عملية الاستعلام هذه. فعلى أي أساس تحصل الحكومة على هذه السجلات؟

نحن في وضع حيث يوجد نوع من الاستيلاء على البيانات بدون وجه حق.

إدارة امن وسائل النقل (TSA) تريد بيانات سجلات اسم المسافر (PNR) من شركات الطيران، وشركات الطيران لا تريد ان تكون جميع بيانات رحلاتها التسويقية بأيدي الحكومة الفيدرالية حيث تشعر شركات الطيران بالحاجة إلى أن تكون المعلومات الخاصة لزبائنها محمية من وصول الحكومة الفيدرالي إليها.

وقالت إدموندز Edmonds (المترجمة السابقة لمكتب التحقيقات الفدرالي وشهدت أمام لجنة 9/11) إن هناك نوعًا من السرعة والارتباط بين جمع البيانات وتحليلها.

وبمجرد حصولنا على معلومات كافية مستمدة من بحث مشكوك فيه، فإننا ننتقل إلى البحث عن Terry.

المعايير:

جادل ادموندز بأن المعايير تتكون من عملية تم استخدامها باستمرار.

إذا وجدنا أنه لا يوجد تفتيش ومصادرة، فيمكن للحكومة أن تضع السياسة بحرية في هذا المجال.

قضية لجنة المراسل:

سجلات الإدانة هي معلومات عامة. وقد حاولت مجموعة من الصحفيين الحصول على مجموعات كبيرة من المعلومات حول سجلات الإدانة، وقضت المحاكم بأن هذه المجموعة واسعة النطاق قد تكون تنتهك الخصوصية.

بعد الامتحان النصفي، سننظر إلى المناطق التي يكون التعديل الرابع فيها غير واضح وكيف يرتبط ذلك بالشفافية.

محاضرة 8: إخفاء الهوية مقابل الشفافية

المحاضر: داني فايتزنر (Danny Weitzner)

الشفافية والمساءلة:

فكر في ذلك كمراجعة لما تمت مناقشته بشأن الخصوصية والمراقبة الإلكترونية. وسيكون لدينا محاضرة تليها جلسة استماع وهمية.

(مرجع برين Brin):

نحن نعيش الآن في عالم يواجه تحديات كبيره في مجال الشفافية. ونحن نحاول أيضًا فهم نوع المساءلة (للآخرين، والجامعات، إلخ) التي يجب أن تكون لدينا اتجاه الآخرين. ونتيجة لذلك، نتجت مفارقه أخرى وهي ان الشفافية الموهومة هذه غير متناقضة مع الأفكار الحالية حول هذا الموضوع.

خطوات:

1. نهاية "أنابيب المداخن" ("The End of "Stove-Pipes"). {من المترجم: يُعد أنابيب المداخن مصطلحًا مجازيًا يشير إلى وظيفة المدخنة كقناة رأسية معزولة، وقد تم استخدامه في سياق مخابراتي بخصوص موضوع تخزين البيانات، لوصف طرق متعددة يمكن تقديم معلومات استخباراتية عبارة عن بيانات أولية خام بدلاً من البيانات المعالجة}.

- أنابيب المداخن (stovepipes) هي مجموعة بيانات مختلفة وهي مستقلة ولا تتقاطع مع بعضها البعض. ومن وجهة نظر الخصوصية، فان هذه الطرق قلصت وحددت من إمكانية وصول الحكومة. تقترب فكرة (أنابيب المداخن) هذه من نهايتها تدريجيا.

2. تكلفة التخزين تقترب من الصفر:

فجوجل تقول لك الآن لا تحذف رسائل بريدك الإلكتروني. وفي السابق، كانت الشركات مهتمة حقاً بسياسات الاحتفاظ بالمستندات التي كانت مدفوعة جزئياً بسياسات مكلفة للاحتفاظ بالمستندات وأيضاً من حقيقة أن مزودي خدمات الإنترنت لا يريدون أن يكونوا مستودعا للوثائق.

- الآن تحتفظ جوجل والشركات الأخرى بكل شيء بدلاً من الانخراط في المساعي المكلفة لمحاولة معرفة ما يلزم حذفه.

3. الاستعلام الرخيص: على مستوى المؤسسة وعلى مستوى الويب:

- أصبح من السهولة القيام باستعلامات على نطاق واسع، فشركتا ياهو وغوغل جعلت هذا العمل متاح. وأصبح من غير المقبول عدم امتلاك ميزة البحث لموقع ويب ما.

4. شبكات استشعار معرفة الموقع/المكان:

- بمجرد أن تقوم بطباعة جزء من البيانات باستخدام علامة الموقع والوقت، يمكنك استخدامه لربط أجزاء أخرى من المعلومات.

كل هذه الأشياء تسبب مشكلة كبيرة لأولئك الذين يشعرون بالقلق بشأن الخصوصية. فهناك خطر حقيقي بشأن الحتمية التكنولوجية عندما نفكر في الخصوصية. ويتم دائما ربط التفكير بالخصوصية بالصور الشخصية.

– مثال على صورة: سجن جيرمي بينيت (Jeremy Benett's Penoptecon). كان يعتقد أن هذا التصميم هو رائع لأنك فقط تحتاج إلى وضع شخص واحد (مراقب) في مكان معين بحيث يمكنه رؤية جميع الأشخاص وجميع الأشياء من ذلك الموقع. وقد كان يُعتقد أن هذه الفكرة هي عن إصلاح السجون، لكنها الآن تشير إلى تمثيل الخصوصية.

– التصاميم الفنية ليست كما تبدو، ومن أجل الخصوصية، علينا التفكير فيما ما تبدو عليه التهديدات والسياسات.

لا ينبغي لنا أن نفكر في أننا يجب أن نفصل أنفسنا عن الآخرين، ونغلق حسابات البريد الإلكتروني والهواتف الخلوية، بل ان التحدي الرئيسي الذي نحتاج إلى مواجهته هو التدخلات في جمع وتنقيب البيانات والتقنيات الأخرى للتعامل مع مجموعه كبيره من البيانات. فنحن نركز كثيرًا على الحد من جمع معلومات الخصوصية والحد من الأدلة، ولكن أعتقد أنه ما يجب أن يقلقنا هو نوع الاستعلامات التي يمكن استخلاصها من الكم الهائل من المعلومات المتوفرة لدينا. وأيضا أي نوع من الضوابط التي نريد أن نضعها للحد من الاعتداء على الخصوصية.

لقد كان قانون الخصوصية وقانون التعديل الرابع بالفعل حول ماهية المعلومات التي يمكن جمعها وليس حول ما يمكن استخلاصه من تلك المعلومات. وتقتضي تلك القوانين أن يحدد جامع المعلومات هدفاً لجمع البيانات ويلتزم بهذا الهدف.

بشكل عام، نحن لسنا جيدين في وضع حدود على الهدف من جمع المعلومات. وهناك قفز مباشر إلى توهم الشفافية.

وسيكون علينا أن نرتاح مع فكرة أن المعلومات مرتبطة بصورة مباشرة بنا وكذلك الاستدلال عليها. قوانين الاستنتاج هي قوانين معقدة.

فهل نحن على استعداد للقيام بسياسة الاستنتاجات التطفلية في جمع البيانات؟

– شخص ما يركب على الطائرة ... ليس إرهابياً، لكنه مدين للضريبة مرة أخرى، وتنتظره دائرة الضرائب بمجرد أن ينزل من الطائرة.

أساسيات القانون الأوروبي هي أن أي شخص يحتفظ بقاعدة بيانات حول معلومات ما يجب عليه أن يسجل تلك المعلومات مع الحكومة، ولكنه ليس هو الحال في الولايات المتحدة، ربما لأننا لا نثق بالحكومة. فانعدام مراكز الثقة في القطاع التجاري في أوروبا هو على عكس الحكومة في الولايات المتحدة.

وهناك مجموعة كاملة من نظرية التشفير يتم تطويرها لتعزيز الخصوصية. (حجب البيانات مثلا).

أحد النماذج التي سنتطرق إليها هو قانون الإبلاغ عن الائتمان العادل (Fair Credit Reporting Act). فالنموذج الذي تم اعتماده لا يحاول التقييد على من لديه المعلومات، ولكن المقايضة هي أن هناك مستويات عليا من المساءلة. تم وضع قانون الإبلاغ عن الائتمان في بداية السبعينيات.

شكل جلسة الاستماع في الكونغرس:

– سيكون لدى جميع الشهود بيانات مكتوبة تقرأها اللجنة. ويجب على كل شاهد إعداد بيان افتتاحي إلى اللجنة لمدة 5 دقائق.

# # # #

تمرين التنميط (ملفات التعريف) والشفافية: المسافر الآمن ياهو (Yahoo Secure Traveler).

مايكل شيرتون (Michael Shirton):

بعد أحداث 11 سبتمبر، تمكنت الشركات التجارية من استخدام هذه المعلومات لتعقب الإرهابيين، فالمعلومات متاحة بالفعل ويمكن الوصول إليها. نحن نريد التخلص تمامًا من عمليات البحث، ونود أن نجعل نظام خطوط الطيران أكثر كفاءة وثباتًا عبر المطارات. هذا سيكون أكثر معيارية.

جيري يودل (Jerry Yodle):

مشاركة أسلوب نقطة ياهو YahooPoint (مخطط السبورة blackboard diagram):

- تتمثل هذه التقنية في حساب الوظيفة الأمنه، حيث يتم إرسال الاسم فقط –ولا يمكن فك التشفير– إلى نقطة ياهو. يتم نقل سجل الاسم الآمن إلى إدارة امن وسائل النقل (TSA).
- هذه التقنية تستخدم أيضا من قبل شركة الطيران الإسرائيلية.

الاتحاد الأمريكي للحريات المدنية (ACLU)

–عمليات بحث واسعة واقل كفاءة.

–هل ينبغي لنا استبدال هذا النظام بنظام ملفات التعريف (profiling system) بالكامل؟

–نحن مهتمون بسلامة الركاب.

–بعض الأجهزة لا يمكن اكتشافها عن طريق نظام ملفات التعريف، وهذا يعرض الركاب للخطر.

–ينبغي تدقيق نظام ملفات التعريف وينبغي أن يكون له قيود صارمة.

–قد تكون غير فعالة حتى تتم الاستشارة وتحتاج إلى مزيد من النظر.

هال ابلسون (Hal Abelson)

- ورقة تأثير كرنفال الكشك (Booth): سيحاول البعض إجراء هندسة عكسية للخوارزمية وسيستهدف الإرهابيون أولئك الأقل عرضة للتفتيش.
- مبدأ كيرتشوف (Kirchoff).
- أي نظام يجب أن يخضع للتدقيق الأكاديمي قبل نشره.

ديفيد فلاير (David Flyer)

- النظام غير آمن.
- الإيجابيات الكاذبة: الأفراد الذين تم تحديدهم على أنهم إرهابيون وليسوا هم كذلك، ولا توجد طريقة للتراجع عن أولئك الذين تم تصنيفهم باستمرار كإرهابيين.
- السلبيات الكاذبة: أسوأ حال! دعوة الإرهابيين للحصول على النظام دون تفحص. فهناك بعض الإرهابيين الذين قد يستفيدون من النظام.
- يمكن أيضا إخفاء الأسلحة في حقيبة الركاب غير المصنفين، ومن ثم استعادة السلاح مرة واحدة على متن الطائرة.

جون غيلمور (Jon Gilmore)

- نظام التفكير غير فعال.

- الشعور بالقلق إزاء مخاطر عدم تفتيش وعدم إخفاء هوية الركاب مع نظام الملفات.

أسئلة من اللجنة:

ما فائدة السماح للأشخاص بالسفر دون الكشف عن هويتهم؟
هذا صحيح. يجب أن يُطلب منك فقط إجراء بحث معقول. ولأجل السفر يعني فقط البحث عن القنابل أو انتهاكات السلامة ... لا أكثر، ولا توجد حاجة للتحقق من المعلومات الشخصية الأخرى.

شيرتون (Shirton)– يجب الحصول على المعلومات. البحث لا يكفي.

إلى الاتحاد الأمريكي للحريات المدنية (ACLU)، ما الذي يجعل النظام غير قابل للمساءلة؟
سجل المسار السابق. يجب حجز الخصوصية للركاب ويجب أن يتم تنظيم المقاول الخاص عن طريق الحكومة. ونود أيضًا مراجعة نظام الخوارزميات جنبًا إلى جنب مع المجتمع الأكاديمي.

كيف نعرف أن سحابة "حساب الوظيفة الآمنة" هي آمنة؟

كيف ستعالج النشرات الدولية؟ في وقت مبكر من عام 2004، خضعت جميع الرحلات الجوية المتجهة إلى الولايات المتحدة لعملية تخليص أمني. هذا من شأنه أيضا أن ينفذ في نظامنا.

البيانات عن طريق شركة تشويس بوينت (ChoicePoint) غير صحيحة بنسبة 63٪ من المصدر في عام 2004. وهذا مقلق وخطير من حيث فعالية البرنامج.

إلى جون غيلمور (John Gilmore):
لكي تبقى مجهول الهوية، هل تقترح أن نقوم بالبحث الجسدي عن كل شخص؟ نعم.

البيانات الختامية:

يعتبر هذا النظام نقطة بداية جيدة، ولكنه بالتأكيد يحتاج إلى تنفيذ إجراءات إضافية لجعل نظام YahooPoint أكثر أمانًا.

توصية لتكامل نظام نقطة ياهو. لا يمكننا إزالة عمليات البحث في هذا الوقت. ولا أعتقد أن النظام سيجعل النظام الحالي أكثر أمانًا، لكنه بدلاً من ذلك يدعو إلى المزيد من النشاط الإرهابي. ويجب أيضًا أن يكون هناك نظامًا للإصلاح يتم تنفيذه في نظام ياهو.

محاضرة 9: المعلومات الشخصية على الويب

المحاضر: هال أبلسون (Hal Abelson)

المعلومات الشخصية على الويب:

1. يمكن للجميع ان يتجسس،
2. ما يمتلكون عنك،
3. وجود معلومات حساسة عنك،
4. سرقة الهوية.

استعمال الكاميرات (للمراقبة) في جامعة جورج واشنطن

نحن نوعًا ما في الوسط فيما يتعلق بالخصوصية. فلم يتطفل عليك أحد بعد، ويمكنك وضع الكاميرات وتشغيلها من خلال برامج التعرف على الوجوه ووضعها على الويب.

أ. كم عدد الأشخاص الذين اعتادوا على التفكير في أنه كان من الممتع البحث في الإنترنت عن خريطة لمنزلك؟

1. كان هذا قبل حوالي 10 سنوات أو نحو ذلك.
2. فلان فعل هذا لشخص لديه معلومات عن جيرانه وتكريماته على الإنترنت، ولقد كانت مرعبة للغاية.
3. طالما كنت بعيدا عن السجلات الطبية وسجلات تأجير فيديوهات التلفزيون التي هي محمية. وهذا يختلف كثيرا عن السياسات في أوروبا.

ب. كم من الناس يعتقدون أن معهد ماساتشوستس للتكنولوجيا يجب أن يضع كاميرات الويب؟

1. هل هناك من فائدة؟ ربما نعم، ربما لا. فقط لإظهار أنه أمر رائع، لنفترض انه لأجل الإعلان أنك يجب أن تفكر في القدوم إلى مدرسة معينة.
2. بعض الطلاب لا يرون مشكلة في استخدام كاميرا ويب واحدة فقط، ولكنهم يرون مشاكل الخصوصية عندما يكون لديك العديد من الكاميرات تتبع حياة الأفراد اليومية.
3. المشكلة تأتي مع الاستخدام غير المتماثل، عندما لا تعلم أنك تخضع للمراقبة. قضايا الشفافية.
4. مشكلة أخرى هي كيفية التقاط الفيديو أو كيفية استخدام كاميرا الويب.
5. أيضا قضية مسألة النزاهة. مثل: تأخير التزود ومعالجة الصور.

ج. برامج التجسس على سطح المكتب:

1. المتلصص على سطح المكتب (Desktop Snooper) – www.snooperspyware.com (من المترجم: الموقع غير موجود الأن، وهذا نبذه عن الأمر: https://archive.org/details/tucows_363037_Desktop_Snooper).
2. قضايا برمجيات التجسس على سطح المكتب:
   i. الكاميرا الخفية التي تنظر في أي حاسوب تختاره.
   ii. السوق يدعي أن هذا النوع من البرمجيات يدور حول حماية أطفالك.
3. آخر الأخبار هو ان برمجية سوني (SONY) تحدد عدد النسخ، وسوني لم تعلمك بأن هذا هو حصل. كما انه أيضا من الصعب جدا إزالة البرمجية.

د. التخزين العالمي لكل شخص (graph–Global Storage per person):

1. قامت لاتونيا سويني (Latonya Sweeney) طالبة دراسات عليا في معهد ماساتشوستس للتكنولوجيا، بتوثيق كمية التخزين اللازمة لتوثيق أنشطة شخص ما، إلخ.
2. في عام 2000، يوجد هنالك تخزين كافي في جميع أنحاء العالم لتخزين المعلومات عن شخص واحد كل 3.5 دقيقة.
3. ماجستير – مجالات في شهادات الميلاد الإلكترونية الآن (1999).
   i. سردت أيضا قوائم الأشياء مثل "عدد مرات إجهاض الولادة".
   ii. سجل ما يصل إلى 226 حقلا لكل حالة ولادة في ماساشوستس.

هـ. كتاب آوهارا (O'Harra)

1. نقاط الاختيار (ChoicePoint).
2. اكسكيوم (Axciom) – يفعل شيئا ما لمساعدة أرباب العمل.

د. أخبار جامعة هارفارد:

1. الطريقة التي تسدد بها هارفارد فواتير الحصول على الدواء هي بطاقة الطالب الجامعية. كما وان الشركة التي استخدمت بطاقات هويات الطلاب تسجل الأدوية التي طلبتها دائرة الخدمات الطبية بجامعة هارفارد.
2. قام اتحاد الطلاب بإجراء دراسة لربط الأسماء مع بطاقات الطالب.
3. تضع الشركة بالفعل معلومات بطاقة الطالب على السيرفر العام. وتدعي الشركة انها لم يفعلوا شيئًا خاطئًا بسبب عدم تحديدهم (عدم كشف هويتهم de–identified).

و. عدم كشف الهوية (De–Indentification):

1. معلومات سرية: تاريخ الميلاد، الجنس، والعرق.
   أ. لا نريد تعميم هذه المعلومات، لذلك يتم إزالة الأسماء.
2. السجلات غير محددة الهوية (De–identified) مع بيانات الرمز البريدي أو الحقول المتداخلة لتضييق إمكانيات سهولة التعرف على هوية فرد ما.
3. تحديد الأفراد بشكل فريد:
   أ. بحث لاتونيا سويني (Latonya Sweeney).
   ب. تاريخ الميلاد والجنس، والرمز البريدي المكون من 5 منازل يحدد بشكل مثالي ما يقرب من 90٪ من سكان الولايات المتحدة الأمريكية.
4. السجلات الجنائية للإحداث في أركنساس:
   أ. استخدام التشفير يؤدي إلى تقليل اختيار الأفراد المحتملين بشكل كبير.

ز. سرقة الهوية:

1. تمرين – التقدم بطلب للحصول علىSSN (رقم الضمان الاجتماعي).
2. تم إنشاؤه لاستخدامه في برنامج الضمان الاجتماعي (1935).
3. في وقت لاحق أصبح SSN معرف "فريد".

أ. أول 3 أرقام تمثل الولاية التي ولدت بها.

- لا تستخدم الأرقام 000 مطلقًا في إنشاء رقم الضمان الاجتماعي.

ب. يُعرف الرقمان ذوي المنزلة 4 و 5 برموز المجموعة: وهذا يشير إلى متى اعتماد رقم SSN

ج. تحديد مشكلة بمعرف الـ SSN:

- يسمح لك بانتحال أو تزييف فردا بسهولة.
- يمكنك شراء رقم ضمان اجتماعي SSN من خلال الموقع: (socialsecuritypeoplesearch.com). كذلك يمكنك الاستعلام عن رقم الضمان الاجتماعي ولكن يجب ان يتوفر لك سبب وجيه للبحث عنه.
- استخدم جوجل للبحث. حيث ينشر بعض الأشخاص أرقام ضمانهم الاجتماعي على مواقع الإنترنت.
- يقوم أساتذة الجامعات بنشر الأرقام الستة الخاصة برقم الضمان الاجتماعي لطلبتهم. مع علاماتهم. وهي فكرة سيئة.
- قاعدة بيانات إدجار (EDGAR).
- قاعدة بيانات SEC: تبين أنه من السهل جدًا العثور على SSN للأثرياء، ومنهم بيل جيت (Bill Gates).

4. هل سجلات الولادة عامة؟

أ. في البحث الحيوي في كاليفورنيا، يمكنك البحث عن سجلات الميلاد التي تتضمن اسم الأم قبل الزواج.

س. قاعدة بيانات سجلات الموتى (SSDI):

1. تبين أن الموتى ليس لديهم أي حقوق.

البنود المذكورة أعلاه كلها موجودة في السجلات العامة ويمكن استخدامها لفحص سرقة الهوية.

ع. لا يفهم الناس كيف تنتشر معلوماتهم الشخصية. هناك فرق بين الصداقة، والصيدلي الجار وبين قواعد البيانات الكبيرة.

ف. هناك انتقال يجب على الحكومة القيام به، ويجب على المستهلكين العمل على إيجاد نظام أكثر أمانًا لتحديد هوية الأفراد. فالنظام الحالي لأرقام الضمان الاجتماعي (SSNs) والمعلومات الشخصية ليس آمنًا كفاية.

بالنسبة لبقية هذا الصف الدراسي، سيكون لدينا هيئة رئاسية تعقد اجتماعًا لحل مشكلة أرقام الضمان الاجتماعي.

تمرين: مؤتمر القمة العالمي حول سرقة الهوية. كيف يجب علينا إصلاح مشكلة الهوية؟

جلسة 1: اتحاد المستهلكين (Consumers Union)، واتحاد الحريات المدنية (ACLU)، إلخ.:

1. من الصعب جداً إثبات أنك لست المنتحل المزعوم، ومن الصعب للغاية تصحيح المعلومات الخاطئة في قاعدة البيانات.
2. المشاكل تنبع من نظام عمره 70 عاما ومن إعادة استخدام SSNs.
3. اقترح إصدارًا معرّف شبيه بـ SSN ويتكون من (10 أرقام) بحيث يترافق مع SSN الحالي. وسيتم إنشاء الأرقام عشوائياً، وترتبط بالبيانات البيومترية ولا ترتبط بالمعلومات الشخصية.
4. المعلومات التي يتعين نشرها، تستلزم الحصول على موافقة أصحابها. وسيتم فرض غرامة بقيمة 1000 دولار على أي منظمة أو شركة لا تلتزم بذلك، وذلك لكل شكل من أشكال المعلومات الشخصية.

الجلسة 2: شرطة ولاية ماساشوستس، ولجنة التجارة الفيدرالية، إلخ.:

1. مشكلة تربك وكالات إنفاذ القانون، وتشكل تهديدا للتجارة بين الولايات.
2. مفتاح USB الذي سيتم منحه مع تسجيل الترخيص.
3. سيكون هذا أفضل لتحديد هوية الأفراد.
4. في حالة فقدان المفتاح، هناك خط ساخن على مدار 24 ساعة للاتصال. وهذا لن يكون مكلفا أكثر من تشغيل خدمة عملاء بطاقة الائتمان.
5. لاستعادة مفتاح USB الجديد، يجب عليك الذهاب إلى وكالة تسجيل السيارات ورخص القيادة (DMV) وتقديم 3 نماذج من تعريف الهوية.

الجلسة 3: التأشيرات، الوثائق المالية والتأمين:

1. جزء لا يتجزأ من تجارة الأمة.
2. تحتاج إلى الوصول إلى بعض المعلومات لتقديم الخدمات بدقة (تقرير الائتمان وتاريخ الميلاد، الخ).
3. اقتراح قاعدة بيانات مركزية ذات معلومات محدودة، مع إبقاء المنافسة مفتوحة.
4. الهدف من قاعدة البيانات هو استخدامها كمرجع والتحقق بشكل صحيح من أن الشخص هو الشخص المقصود.
5. طرف آخر سيحافظ على قاعدة البيانات.

الجلسة 4: eBay و Amazon و WalMart وغيرها من القطاعات الخاصة:

1. يجب أن يكون نظام المعرف الجديد رخيصًا وفعالا. ولا نريد أن ندفع نحن ولا المستهلك ثمنها.
2. أولئك الذين يصدرون المعرف يجب أن يدفعوا مقابله.
3. لا نريد قوانين مقيدة حول كيفية مشاركة البيانات.
4. بالتقريب، فان النظام جيد كما هو موجود. وأي حلول جديدة يجب ألا تضر بالقوة الشرائية للمستهلك ولا بأرباحنا.

الجلسة 5: شركات Equifax و Experian و Acxiom، وغيرها من صناعة سجلات التوظيف والتدقيق الأمني:

1. كل فرد لديه بطاقة التشفير والتي لديها معرف الشخصية حيث يطلب منهم التوقيع.
2. طبقتين من الأمن:

(1) لا أحد يعرف المعرف الشخصي في البطاقة، و (2) إذا سرقت البطاقة، فعليك الإجابة عن السؤال السري.

3. الحكومة ستصدر البطاقات. ويجب أن يكون لديك 3 نماذج منفصلة لتعريف الهوية (على غرار الحصول على رخصة القيادة).
4. هذا يساعد على دقة وأمن المعلومات.
5. على استعداد لخسارة بعض المال من أجل الحصول على الأمن.

مخاوف أخرى:

1. تغيير الأسماء دون سرقة الهوية.
2. التغييرات في الهوية الفيزيائية (الجسدية).

حدث مداولات في اللجنة.

محاضرة 10: الشفافية في حماية المستهلك والتنظيم التجاري

مكرر عن محاضرة 9 من المصدر.

محاضرة 11: أصول تنظيم البث

المحاضر: هال أبلسون (Hal Abelson)

الجنس، والمخدرات، وموسيقى الروك والرول (كيف يصبح المجاز قانونا: أصول تنظيم البث).

تركز هذه المحاضرة في الغالب على تاريخ وتنظيم الاتصالات والاستعارات التي شكلت هذا القانون والتكنولوجيا من خلفه.

أولا) المخدرات:

أ. أغنية نفخة التنين السحري (Puff the Magic Dragon). لا يتم تشغيلها في عام 1971.
{ من المترجم: هي أغنية كتبها ليونارد ليبتون وبيتر يارو، وقد أصبحت شعبية لدى مجموعة يارو بيتر وبول وماري في تسجيل عام 1962 صدر في يناير 1963. بعد النجاح الأولي للأغنية، نشأت التكهنات – في مقال نشر عام 1964 في مجلة نيوزويك – بأن الأغنية تحتوي على إشارات ضمنية لتدخين الماريجوانا }.

ب. لجنة الاتصالات الفدرالية (FCC) انتقلت إلى "الخبراء" (الجيش الأمريكي) بعد انتشار الموسيقى الشعبية لترويج المخدرات.

ج. 27 أغنيه لم يتم تشغيلها ضمن القائمة:
1. تم الطلب من الكليات (والصحف، والمنظمات) عدم تشغيل هذه الأغاني في قائمة التشغيل.
2. دعوى قضائية قدمت ضد جامعة ييل (Yale) وخسرت.

ثانيا) الوسائط التي تم تنظيمها:

أ. البث الإذاعي والتلفزيوني،

ب. الكتب والصحف،

ت. العم فيستر {من المترجم: العم فيستر – شخصية تلفزيونية خيالية بأوصاف غريبة):
1. لا تتذكر الاسم الحقيقي،
2. كتب عن كيفية تصنيع الميثامفيتامين أو الميث (methamphetamine وهو نوع من أنواع المخدرات المنشطة) ونشر كتابة – أشياء سيئة.

د. حاولت الحكومة معرفة أين يجب أن تكون الإنترنت مناسبة:
1. التكنولوجيا الجديدة تقدم قوانين جديدة، لذا فإن الاستعارات تنتهي بها المطاف إلى أن تصبح قانونًا،
2. من 1995–2001 تحولت الاستعارة من الأسلحة إلى الحماية من الاحتيال على بطاقات الائتمان وتكنولوجيا التشفير.

ثالثا) قوة الاستعارة في تنظيم البث:

– التفكير في السياسة الحقيقية بالتزامن مع كيفية مواكبة تطور التكنولوجيا والقوانين.

أ. غرق سفينة التايتانيك (15 أبريل 1912):
1. بداية الراديو. لقد كانت البحرية تستخدم الراديو للاتصالات،

2. البحرية كانت مستاءة جدا بسبب المتسللين وشركة ماركوني (Marconi شركة تلغراف لاسلكي)،
3. ماركوني – مصلحة تجارية تخص التلغراف اللاسلكي، حيث اشتكت الشركة من أن الأعمال تتعرض للأذى من قبل محطات خارجية غير منظمة،
4. غرقت سفينة التايتانيك، ونجت غرفة راديو واحدة بشكل سليم،
5. كانت سفينة الكارباتيا (Carpathia) على بعد 10 أميال من سفينة التايتانيك، ولكن لم يكن مطلوبا من مشغلي الراديو ان يكون الراديو مفتوحا طوال الوقت.

ب. أعمال الكونغرس:

1. مواءمة المصالح العسكرية والتجارية،
2. المصلحة العامة الضخمة،
3. جلسات الاستماع بواسطة وليم سميث (William Alden Smith) والذي قرر أن الكارثة الحقيقية (في غرق سفينة التايتانيك) كانت في عدم وجود اتصالات لاسلكية،
4. اقترح سميث أن على الكونغرس سن لوائح الراديو وساعد على تفعيل قانون الراديو لعام 1912.

ج. قانون الراديو لعام 1912، وتضمن:

1. تستخدم كارثة سفينة التايتانيك لتشمل موجات الهواء،
2. لا يمكن لأحد ان يقوم بالبث بدون رخصة،
3. الترددات المسموح بها،
4. العسكرية حصلت على ترددات ممتازة،
5. الشحن التجاري والاستخدام التجاري،
6. تم حظر الهواة من الترددات "المفيدة" وتم تنظيمها إلى الترددات التكنولوجية غير القابلة للاستخدام.

د. قانون ما بعد الراديو (Post Radio Act):

1. فترة 1914–1918 اعتبرت السنوات الذهبية،
2. 1919– تم تشغيل الراديو باحتكار من قبل الحكومة،
3. أصبح هوفر (Hoover) مهتمًا بالبث وإقامة فرقة للإذاعة التجارية،

{من المترجم: في السنوات الأوائل من البث الأمريكي، أثر وزير التجارة الأمريكي هيربرت هوفر (Hoover) تأثيرا عميقا على تطوير البث الأمريكي، في الواقع، كان "هوفر" أول من نشر معيار المصلحة العامة في البث الأمريكي.}

4. 1920– تم بث الانتخابات الرئاسية،
5. 1921 – تم بث المباريات العالمية. كانت هناك 5 محطات إذاعية في الولايات المتحدة،
6. 1922 – كان هناك 576 محطة إذاعية وكانت مساحة النطاق العريض ممتلئة، ولهذا قام "هوفر" بتوسعه مساحة النطاق،
7. دعوى قضائية ضد راديو انترستي (Intercity) وذلك بسبب رفض الترخيص، وخسر هوفر القضية،
8. قضت المحاكم بأنه ليس لديها سوى سلطة تنظيم ممرات الشحن التي لا تختار من يستطيع استخدامها، لذلك تم توسعة النطاق مرة أخرى.

هـ بث الطيف الراديوي:

1. تحدث هوفر عن ذلك "بانه من الأصول الوطنية الكبيرة" و "مصلحة عامة لكي نقول من الذي سيقوم بالبث"،

2. خلاف في التردد بين زنث (Zenith) و ج.اي. (GE):
   - حولت الشركات البث إلى التردد الكندي ولم يتم فرض عقوبات،
   - رفعت قضية وتم كسبها.
3. 1926 – المحكمة حكمت حكما قاسيا على "هوفر" بشأن سلطة تنظيم البث،
4. 1927 – فوضى الراديو. "هوفر" أصبح خارج مجال تنظيم العمل.

و. قانون الراديو لعام 1927:

1. ان الكونغرس يمرر قوانينه الخاصة وتشريعاته ويتم اعتبارها كمبدأ للبث،
2. أصبح الطيف مملوكًا للجمهور حاليًا ويخدم المصلحة العامة. ويرخص من لجنة الإذاعة الفيدرالية (FRC)،
3. قانون الاتصالات لعام 1934 حل محل القانون السابق، وFRC أصبح FCC،
4. القانون كان نتيجة لتفادي التداخل لأن الطيف كان مصدرا للقلق، ولهذا عملت الحكومة على احتكار البث الإذاعي،
5. معيار المصلحة العامة – على الرغم من أن التنظيم القوي، فانه لن يتعارض مع حرية التعبير ولن يتم بث أي محتوى مهين.

رابعا) الجنس:

ز. جون رومولوس برينكلي (John Romulus Brinkley) يزعم انه طبيب:

1. اشترى درجة (شهادة) في الطب من جامعة في ولاية كانساس،
2. فتح مجال ممارسة وملاحظة الماعز المرح (Frisky Goats)،
3. برينكلي زرع خصية الماعز في مريض يعاني من ضعف الانتصاب،
4. 1923 – بدء بتشغيل محطة الراديو (KFKB) (كانساس الأولى، كانساس الأفضل):
   - بث عمليات زرع غدة الماعز وقدم المشورة الطبية،
   - كانت المحطة الأكثر شعبية في عام 1930 (4 أضعاف)،
   - الجمعية الطبية الأمريكية كانت غير سعيدة بشعبية المحطة.
5. في عام 1930، فقد برينكلي رخصته الطبية وترخيص البث من لجنة الاتصالات الفدرالية (FCC)،
6. حكمت المحكمة ضده، وقالت لجنة الاتصالات الفيدرالية (FCC) على أنه نظراً لضيق الترددات، يجب مراعاة طبيعة الخدمة المقدمة وجودة الخدمة لذلك تم إلغاء الترخيص،
7. سافر إلى المكسيك لممارسة مهنته وترشح لمنصب حاكم كانساس،
8. كان هذا هو نشأة تنظيم البث والقضية المرفوعة للمحكمة من شركة البث الإذاعي الوطني (NBC) ضد الولايات المتحدة.

ح. شركة البث الإذاعي الوطني (NBC) ضد الولايات المتحدة:

1. تنظيم أكثر صرامة للبث لأنه محدود، ويختلف عن طرق التعبير الأخرى مثل الكتب والطباعة حيث يكون الاستجابة فيها محدودة أيضًا،
2. البث الإذاعي لـ (Red Lion) ضد لجنة الاتصالات الفيدرالية (FCC):
   - وقت الاستجابة متساوي.
3. ان الطيف (Spectrum) ليس كبيرا بما يكفي لاستيعاب الجميع – ثبت في وقت لاحق أنه خطأ.

ط. الأرض:

1. الحكومة تمتلك الموارد الطبيعية (مثل نظام المتنزهات الوطنية)،
2. استعارة – تنظيم البث والإذاعة قد ظهرت وهي تشبه التنظيم الحكومي لنظام المتنزهات.

ي. الإنترنت:

1. وجود أنواع مختلفة من التواصل الإعلامي أدى إلى التصادم مع بعضها البعض.

ك. هيدي لمار (Hedy Lamaar):

1. ولدت في عام 1914 وكانت ممثلة في سن الطفولة،
2. في سن الـ 19، كانت أول امرأة تظهر عارية في فيلم روائي طويل،
3. وكانت تعمل مضيفة لحفلات ماندل (Mandl) في فيينا وترحب بأصدقائها من رجال الأعمال،
4. كان الزوج ماندل غيور للغاية، وفي وقت لاحق هرب إلى لندن وطلق ماندل،
5. لويس ماير (Louis Mayer) وهوليوود:
   أ. التقى لويس بهيدي في لندن وأخذها إلى هوليوود، حيث انه فوجئ بجمالها.

ل– جورج انشيل (George Antheil):

1. كان الطفل معجزة والراعي كان هو كريس باخ (Chris Bach) (؟)
2. لقد أصبح المؤلف الشهير جدا في 1920،
3. التكوين الأكثر شهرة – يتألف من لاعب البيانو والمراوح الطائرة،
4. كتب تأليفات أفلام جون وانغ (John Wang)، وغيرها،
5. وفي هوليوود، قام بتأليف نظام "See–Note" للنوتات الموسيقية،
6. هو مهتم فعلا بعلم الغدد (الصماء).

م. لقاء لمار وأنثيل (Lamaar and Antheil):

1. في عام 1940 التقيا في حفل عشاء في هوليوود،
2. سألت لامار عن الهرمونات وتضخم الثدي،
3. كانت لامار تريد ترك هوليود وتريد أن تقدم خدماتها إلى المجلس الوطني للمخترعين،
4. كلاهما كان وطنيا جدا وأرادا أن يساعدا في المجهود الحربي. وأرادت لممار معرفة المزيد عن الطوربيدات،
5. تم التحكم في الطوربيدات بواسطة الترددات، والسفن نريد التنصت لمعرفة إمكانية القضاء على طوربيدات العدو،
6. كان لدى لامار فكرة لتحويل الترددات لمنع التشويش على الطوربيد،
7. كان لدى أنثيل حل من خلال استخدام مفاتيح البيانو للتحكم في قفزات التردد.

ن– مصير الاختراع

1. منح لامار وأنثيل براءة اختراع إلى البحرية، لكن لم يتم تطبيقها، وذلك لانهما كانا يعتقدان ان تنفيذ الفكرة بحاجة إلى وضع عازف بيانو على الطوربيد،
2. في عام 1950، أصبح التحكم الإلكتروني ممكنًا،
3. تم استخدامه بكثافة في ازمه الصواريخ الكوبية عام 1962،
4. في عام 1997، تم تكريم لامار وأنثيل بجائزة الرواد لعملهما.

ص– مسابقة لكورال درو (Corel Draw)

1. كان الدخول للفوز هو عبارة عن صورة عن لامار ويتم إنشاؤها باستخدام برمجية Corel 8،
2. قامت لامار برفع دعوى قضائية بمبلغ 15 مليون دولار ضد المسابقة ولكنها تلقت مبلغ 5 ملايين دولار.

كل التاريخ والاختراعات قامت على الاستعارات، والآن نحن نعتبرها أمرا شائعا، لكن الاستعارات ليست حقيقية. ونحن مشغولون في اختراع وإعادة اختراع هذه الاستعارات عبر الإنترنت والتكنولوجيا الجديدة.

ولدينا الفرصة للنظر إلى أبعد من هذه الاستعارات وخلق استعارات جديدة.

المحاضرة 12: تحديات السياسة العامة على شبكة الويب الدلالية (Semantic Web)

المحاضر: داني فايتزنر (Danny Weitzner)

تحديات السياسة العامة على الويب الدلاليّة: الخصوصية، والمنشأ، والممتلكات، والشخصية.

اليوم سنقضي الوقت في مناقشة العمل الذي شارك به كل من هال وداني (Hal and Danny) بالإضافة إلى موضوعات سنناقشها في هذا الفصل. وسنبحث أيضًا منظور السياسة العامة حول البنية التحتية للإنترنت وكيف أثر ذلك على تصميم شبكة الويب (WWW).

أولا) نظرة عامة:

أ. قضايا الخصوصية،

ب. الملكية،

ج. المنشأ/المصدر: من أين تأتي المعلومات، وإذا كان علينا ان نثق بها أم لا.

(رسم بياني على الشريحة 4) / غير موجود من المصدر.

ثانيا) فلسفة شخصية:

أ. التكنولوجيا هي فوضى،

ب. نظرة عامة: يحتاج القانون إلى اللحاق بالتكنولوجيا.

ثالثا) قوانين:

أ. نحن نفهم فقط ما يجب القيام به (مثل اللغات) والتي غالبا ما نتبعها معظم الوقت، ونقوم بعمل الشيء الصحيح دون أن تكون هذه القوانين صحيحة أمامنا.

ب. شبكة الإنترنت غريبة بالنسبة للقوانين:

I. نحن نشتري ونبيع دون معرفة الأطراف، ولا نعرف بسهولة الخصوصية والحماية التي نتمتع بها،

II. طبيعة الويب لا تجعل معرفة القوانين علينا سهلة،

III. التكنولوجيا تساعد البيئات على التكيف حتى نتمكن من معرفة ما يجب القيام به وما لا يجب فعله،

IV. الكثير مما حاول الناس القيام به هو "حواجز لإنفاذ سياسة سابقة" وذلك لمنع الناس من القيام بأنشطة أو لفرض قواعد معينة،

V. يجب أن يكون التركيز على إبلاغ المستخدمين بكيفية الالتزام بالقواعد بدلاً من منعنا من القيام بتلك الأعمال.

رابعا) تحولات الخصوصية:

أ. يجب أن تستند معظم التدخلات التي يجب أن نهتم بها على الاستدلالات المأخوذة من الحقائق وليست من الممارسات والمعلومات التي تم جمعها.

ب. أمثلة:

I. معاملات بطاقات الائتمان والملفات الشخصية،

II. سجلات تسجيل الدخول إلى الويب وأنماط البحث على شبكة الويب،

(أصبح الناس أكثر اهتمامًا بكيفية استخدام الأشخاص لسجلاتهم وكيف يبحثون في الويب، تأمل جوجل)،

III. الموقع اللحظية وأنماط السفر.

ج. هناك عدد قليل جدًا من حواجز الجمع في الولايات المتحدة، ولكن مع المزيد من التركيز على وضع القواعد للعمل بها فيما يتعلق بكيفية استخدامنا للبيانات ووصف الاستخدام مع المساءلة، فنحن في الواقع لم نتخذ قرارًا بشأن جوهر الموضوع:

I. رابطة صناعة التسجيلات الأمريكية (RIAA) – قواعد بعد الحدث (after the fact) لتحميل الموسيقى.

خامسا) المنشأ/المصدر:

أ. المنهج المركزي – بما أن الصحافة الحديثة تمتلك آليات مركزية لكيفية مشاركتنا للمعلومات ولمواد التحرير:

I. الصحيفة – يمكن فلترة "تصفية" عناوين المواضيع التي يتم نشرها في الأخبار،

II. جوجل – خوارزمية البحث:

– لقد أثرت فعلا في كيف نرى للعالم،

– ولربما لم تؤثر أي مؤسسة أو منظمة مركزية أخرى مثل هذا التأثير على العالم أكثر من تأثير الدين.

ب. النهج اللامركزي – الأخبار على الإنترنت:

I. تسمح لك بمشاهدة البيانات المنظمة والبيانات الوصفية،

II. يمكن تطبيق مرشحات الثقة (Trust Filter) من أجل تصفية المعلومات {من المترجم: مرشحات الثقة تقوم بفلترة وتصفية المعلومات بناء على معايير معينة وعلى رغبة المستخدم}.

III. بعض المتصفحات تسمح لك بجمع مجموعة من البيانات ثم تصفيتها (خلافا لنيويورك تايمز)،

IV. موقع (del.icio.us):

{من المترجم: موقع يقدم خدمة مجانية لحفظ روابط الويب التي يجدها المستخدم مفيدة عبر الويب ويقوم بتنظيمها وتذكرها}.

– يستخدم المنهج اللامركزي لمشاركة نتائج البحث،

– ويمكنك اختيار وجهة نظر شخصية لما ترغب في رؤيته أو جهة البيانات التي تثق بها،

لذلك هناك خروج من فكرة المرشحات المركزية إلى المرشحات التي تحدث بطريقة أكثر توزعا.

سادسا) الملكية:

أ. ظهور مفاهيم جديدة حول كيفية حماية الملكية الفكرية سواء من الناحية الفنية أو القانونية.

ب ظهور نموذج جديد لإنتاج المحتوى:

I. من محتوى هوليوود الحالي (الإنتاج المركزي) إلى المحتوى اللامركزي الذي نستخدمه (مثل خدمة مشاركة الصور في فليكر Flikr، ومدونات الويب، إلخ.)

II. رخص المشاع الإبداعي (الرخص الحرة لاستخدام المحتويات) – وصف مفتوح لشروط الترخيص على أمل أن يتبع الناس هذه القواعد. جوجل وياهو تسمح لك الآن باستخدام ترخيص المشاع الإبداعي لتصفية بياناتها أثناء البحث.

III. مرة أخرى تتحول حواجز التنفيذ إلى معلومات مفتوحة وإلى المشاركة على شبكة الإنترنت.

سابعا) نموذجين اثنين من الشخصنة/ الشخصية (Personhood):

– توجد ثغرات كبيرة في إدارة الهوية عبر تكنولوجيا الإنترنت.

أ. حاولت شركة ليبرتي الليانس (Liberty Alliance) وشركة صن ميكروسيستمز (Sun Microsystems) معا إنشاء نظام موثوق ومعتمد للهوية:

1. حزم معلومات تعريف الهوية (ID) المتعدد، حتى يمكن أن يكون هما للطرف الثالث "الموثوق"،

2. ينكن اعتباره هذه الحزم معقدة للغاية/ ويصعب معرفة ما إذا كان يتم العمل بها أم لا.

ب. النهج اللامركزي:

1. قابلية الإسناد لمحتويات المؤشرات (De-referencerable) للطرف الثاني.

ثامنا) خاتمة:

أ– التحول من أنظمة مركزية إلى أنظمة لامركزية أكثر،

ب. الاعتقاد ان القواعد في هذا الوضع ستكون أكثر وضوحا للناس، مما يؤدي إلى المزيد من الأشخاص الذين يتبعون القواعد.

ج–الحاجة إلى مزيد من الشفافية لهذه القواعد مع القدرة على ضبط أولئك الذين يخالفون هذه القواعد.

ملحق بالمحاضرة 6: حرب التشفير

(من المترجم: نصوص مشفرة):

....

FNNC ZESDQMNNM !

Sghr kdbstqd hr
zants dmbqxoshnm

الخطوط العريضة - موجز

- **الجزء الأول: التشفير، ما قبل عام 1970:**

– يوجد الكثير من التشفير قبل تاريخ بدء الإنترنت له علاقة بالتشفير في الوقت الحالي.

- **الجزء الثاني: المفتاح العام التشفير:**

– تكنولوجيا الاختراق الرئيسية.

- **الجزء 3: مناقشة سياسة التشفير 1990–2000**

– دراسة حالة لضغوط السياسات الناجمة عن التكنولوجيا.

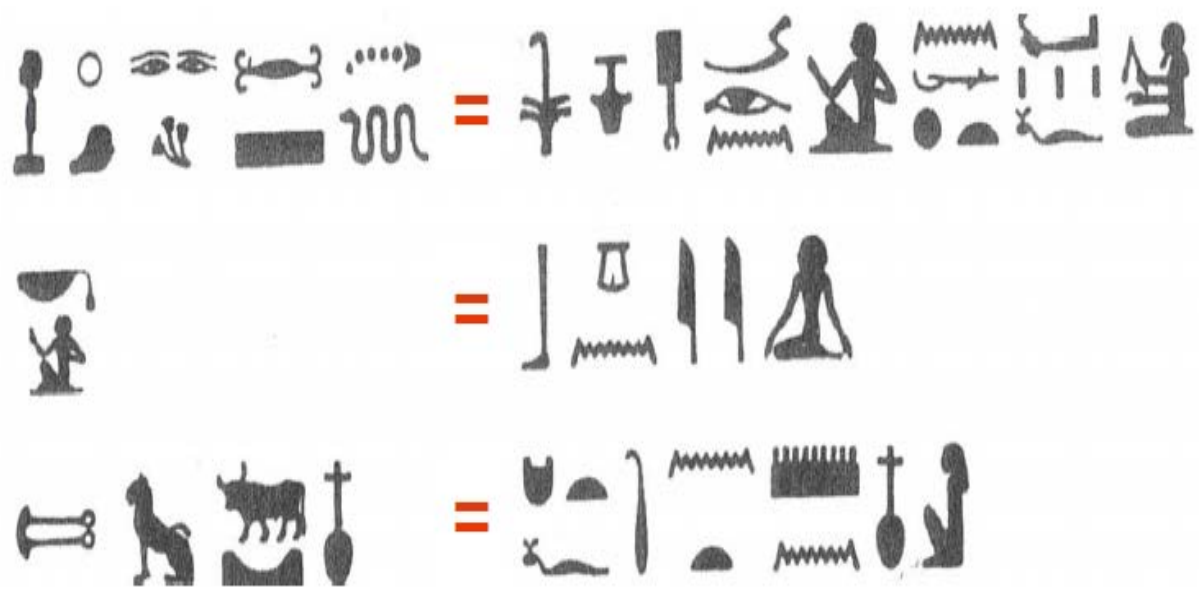
الاحتياجات السرية في الشبكات

- **السرية** (Confidentiality): الأشخاص المصرح لهم فقط، على سبيل المثال، المرسل والمستلم للرسالة، ولا يمكن لأي متلصص معرفة الرسالة.

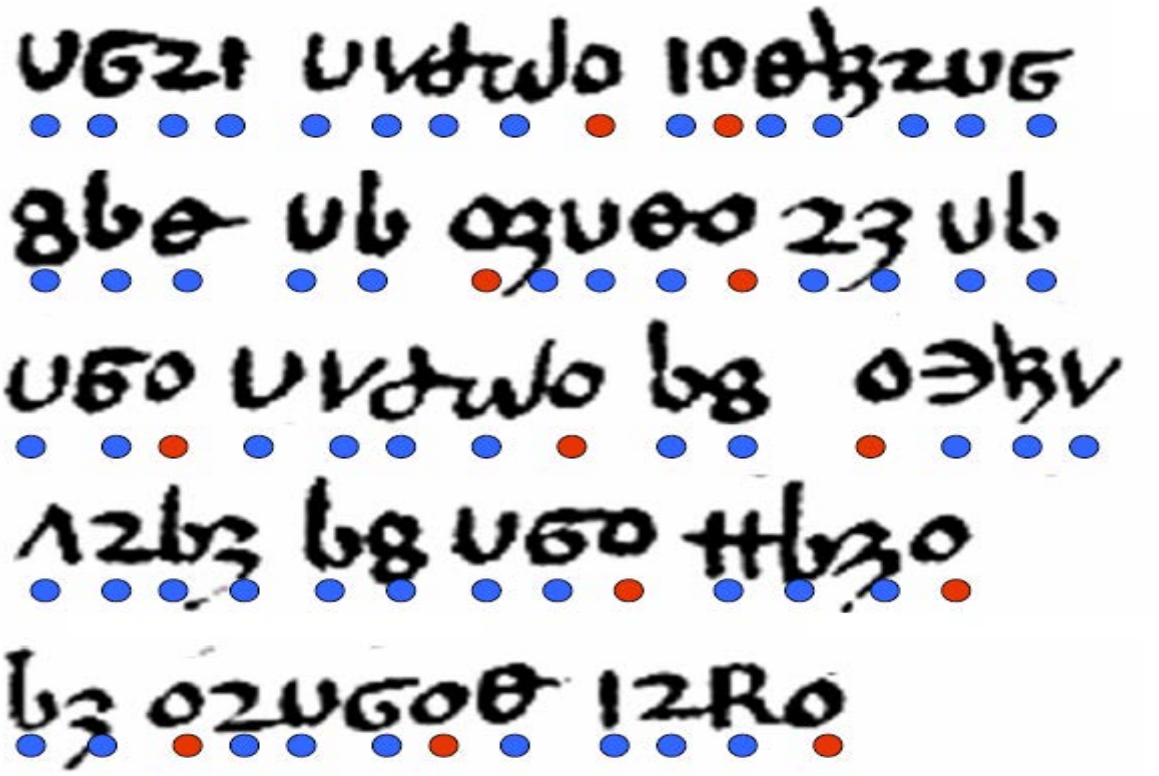
نفذت باستخدام التشفير

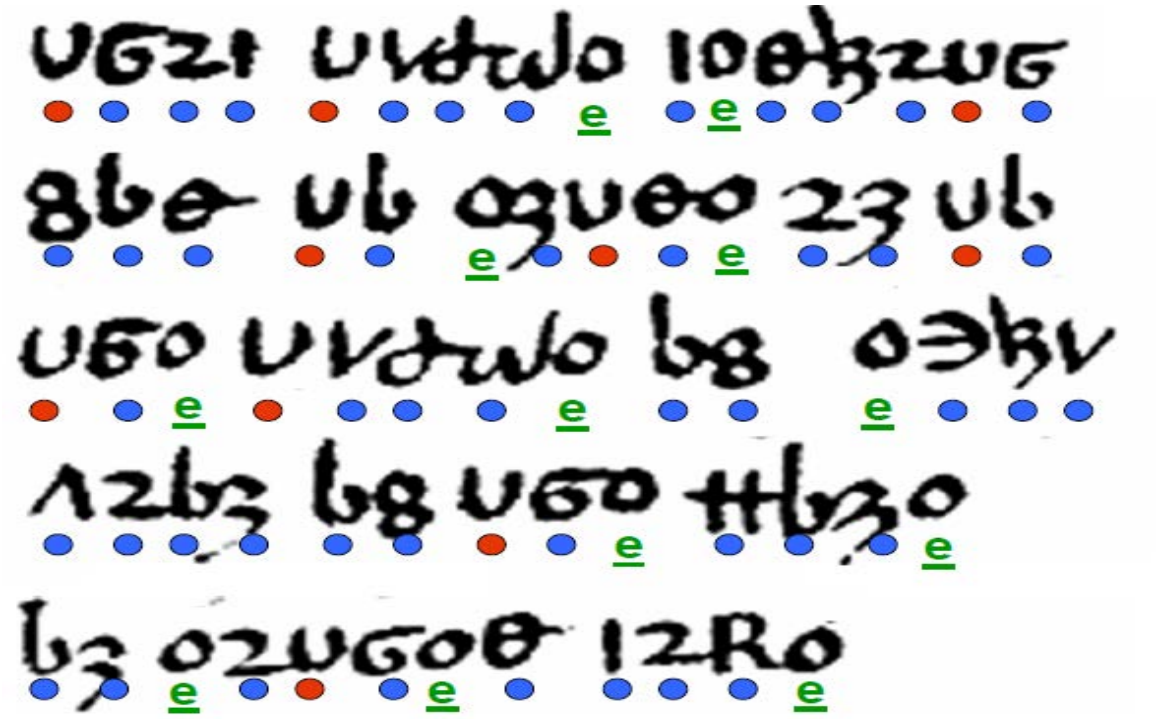
- **المصادقة** (Authentication): عندما يتلقى بوب (Bob) رسالة تفيد أن هذه الرسالة تم إرسالها من قبل أليس (Alice)، فانه هذه المصادقة تعني ان بوب يمكنه التأكد أن هذه الرسالة تم إرسالها **فعلا** من أليس.
- **النزاهة** (Integrity): عندما يتلقى بوب رسالة، يمكنه التأكد من أنه لم يتم تعديلها خلال إرسالها بعد أن أرسلتها أليس.
- **عدم التنصل** (Non-repudiation): أي عدم الإنكار بحيث لا تنكر أليس في وقت لاحق أن الرسالة تم إرسالها، كما لا يستطيع بوب أن ينكر لاحقًا أن الرسالة تم تلقيها.

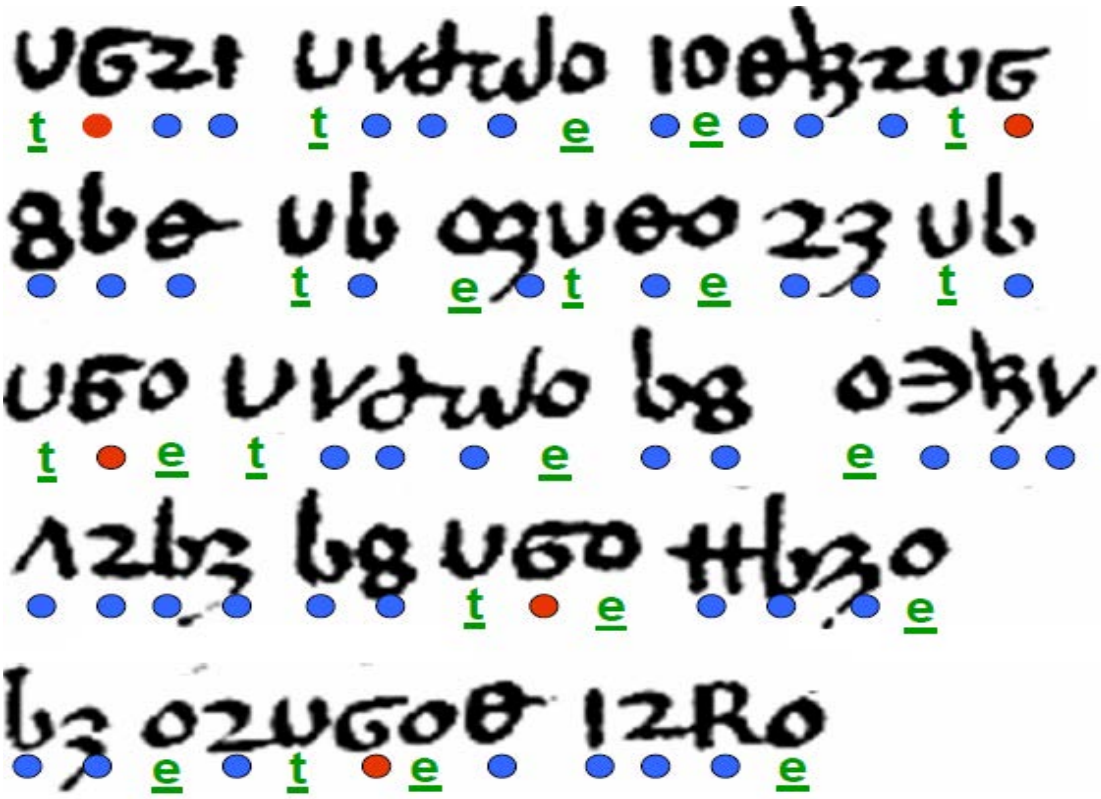
التشفير، 1900 قبل الميلاد

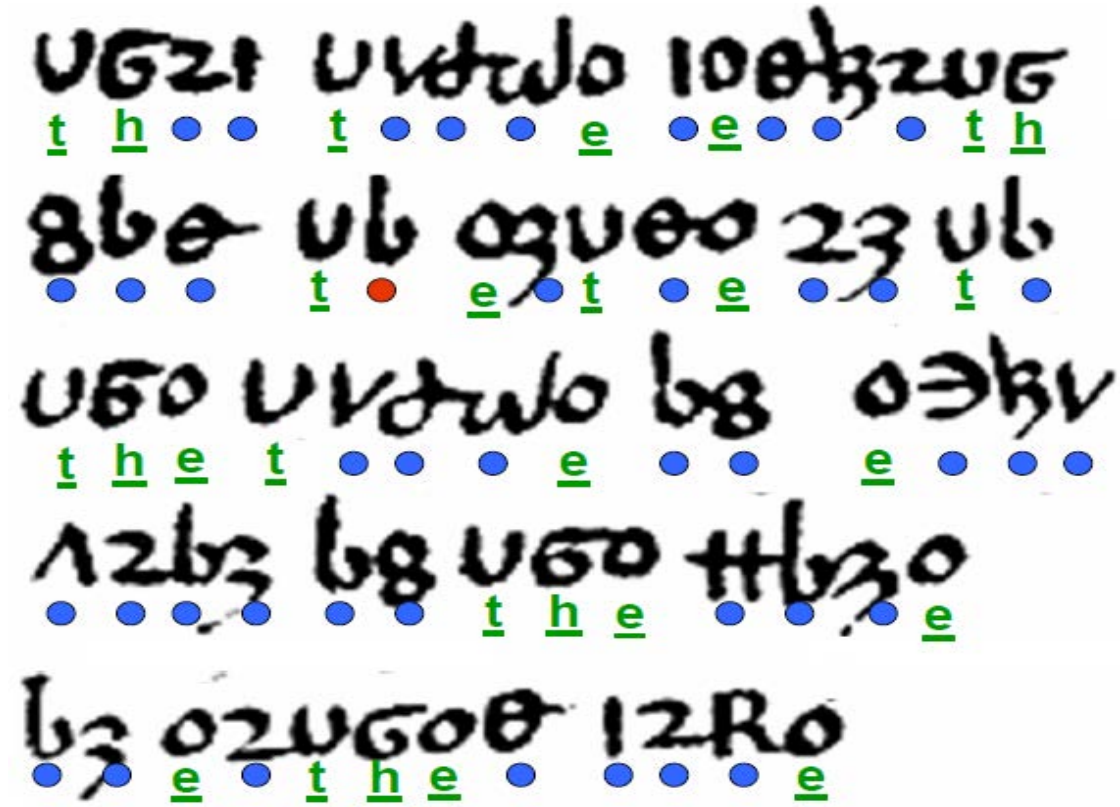


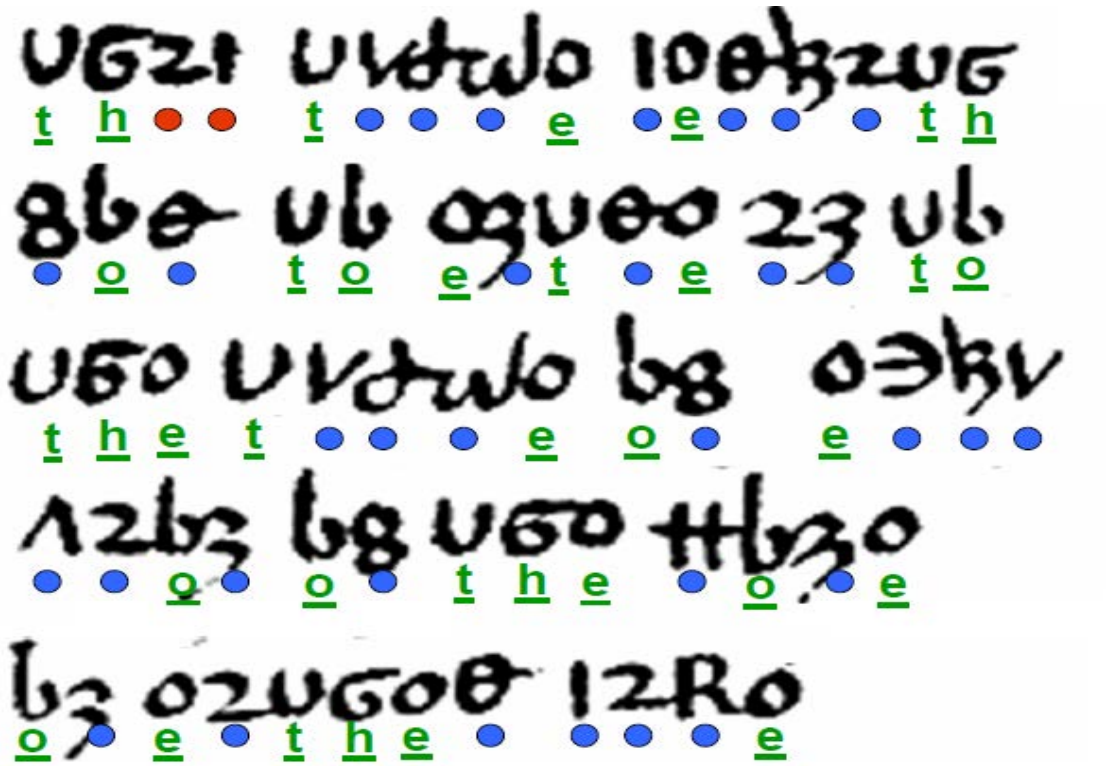
جيفري شوسر (Geoffrey Chaucer)، أطروحة عن الأسطرلاب، 1391

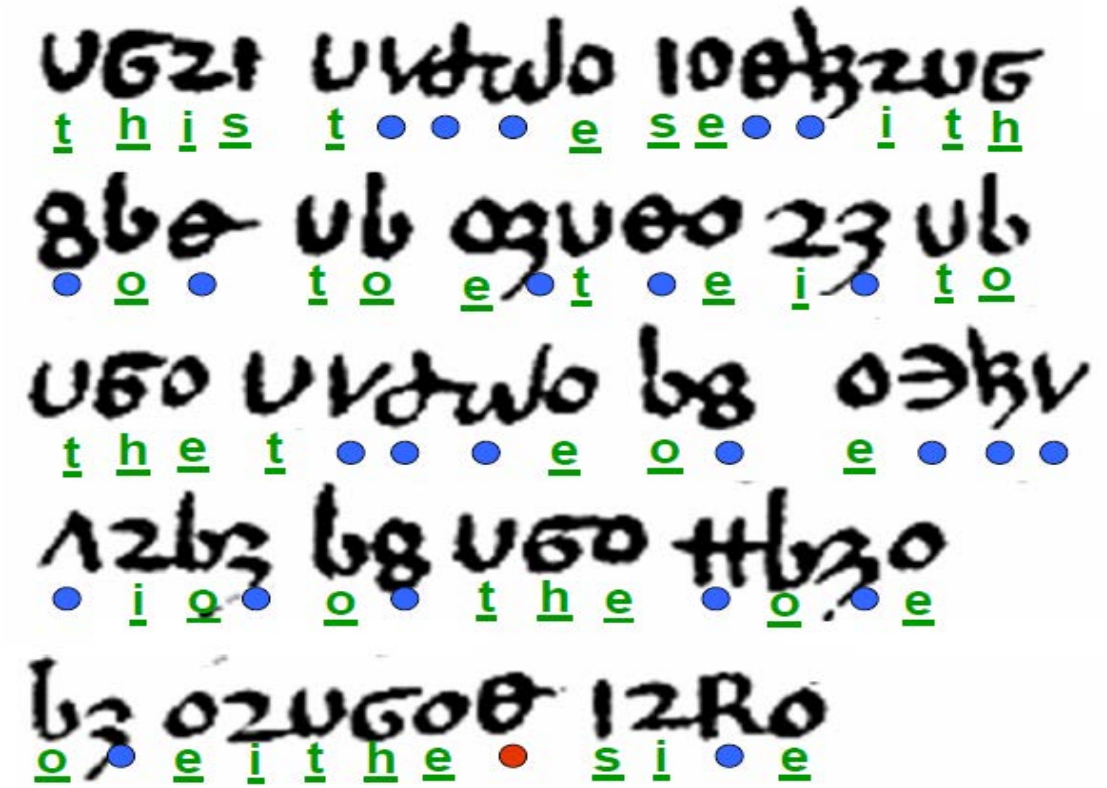


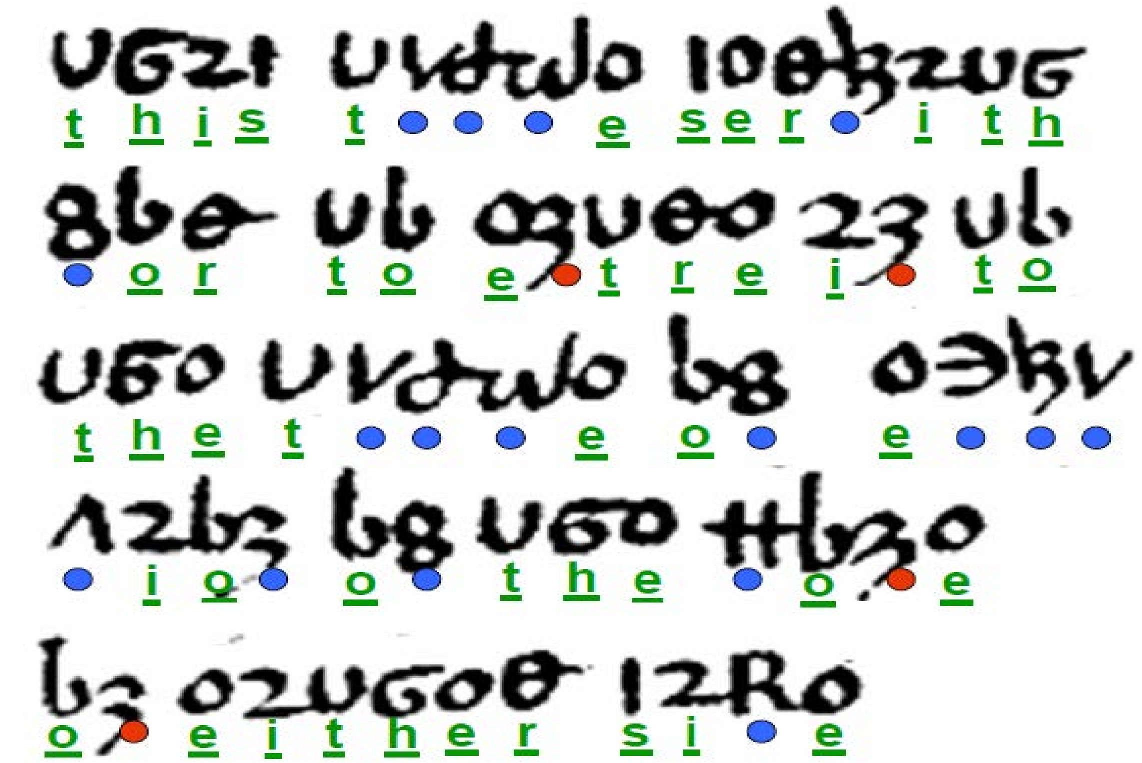


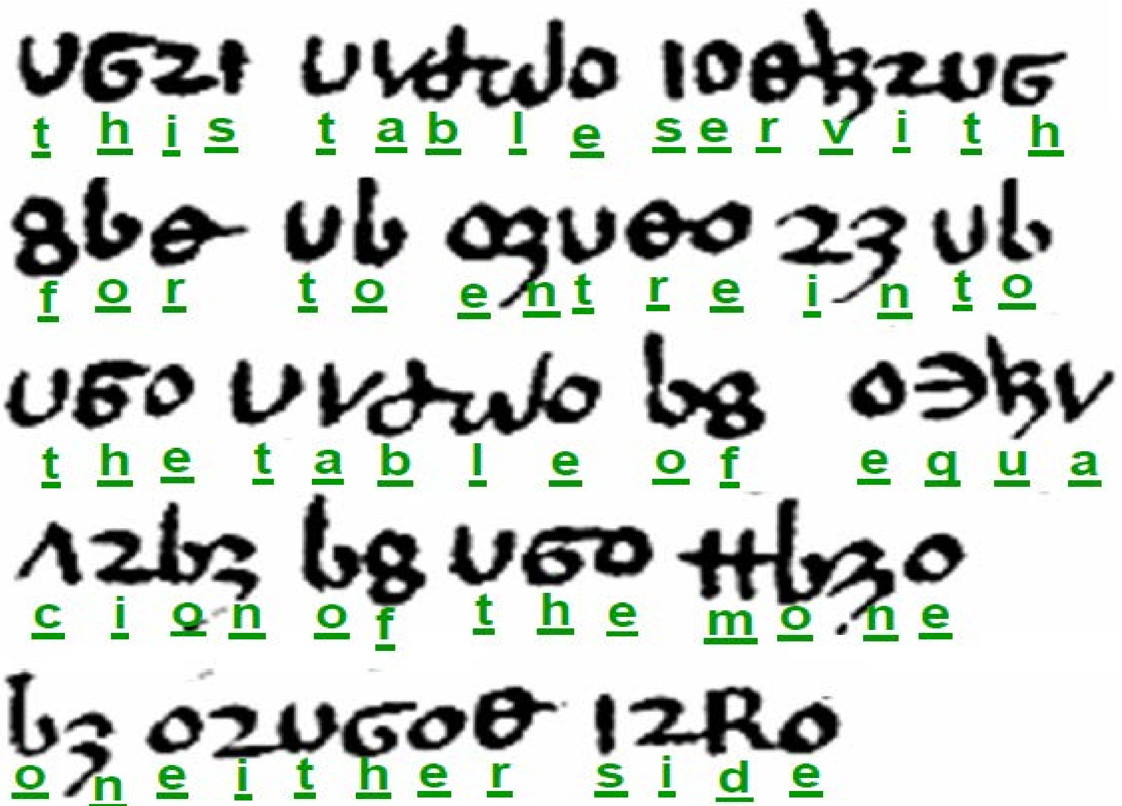









t h i s t e s e r i t h
o r t o e t r e i t o
t h e t e o e
i o o t h e o e
o e i t h e r s i e


t h i s t a b l e s e r v i t h
f o r t o e n t r e i n t o
t h e t a b l e o f e q u a
c i o n o f t h e m o n e
o n e i t h e r s i d e

شفرة الاستبدال (Substitution Cipher)

هذه الطريقة تقوم بالآتي:

- استبدل كل حرف في الرسالة بحرف آخر، وفقًا لبعض القواعد،
- الاستبدال البسيط أو الاستبدال الأحادي (Mono–Alphabetic Substitution): يتم استبدال كل حالات التكرار لرمز ما في الرسالة بنفس الرمز.
- بشكل عام:

– تسمى الرسالة الأصلية بالنص الصريح أو العادي (Plaintext).

– تسمى النتيجة المشفرة بالنص المشفر (Ciphertext).

شفرة القيصر (Caesar cipher)

ويتم فيها استبدال كل حرف بالحرف الذي يأتي قبله أو بعده وذلك بناء على مسافة ثابتة في الأبجدية.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

التحريك=3

النص الصريح **Galliain tres partes divisa est Omnia**

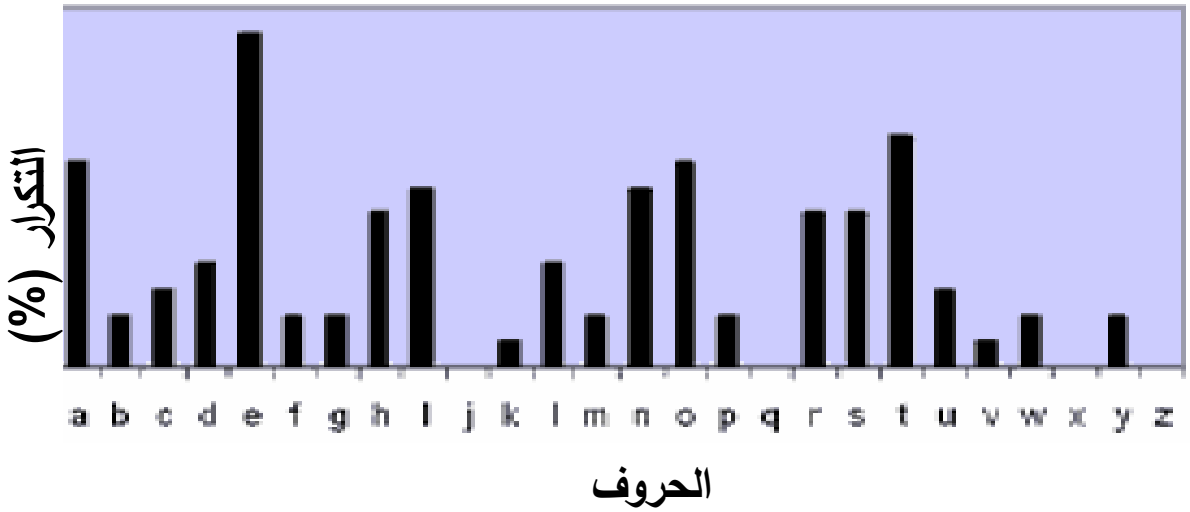
النص المشفر **LJKF XDXI IFXF KQOB PMXO QBPA FSFP XBPQ**

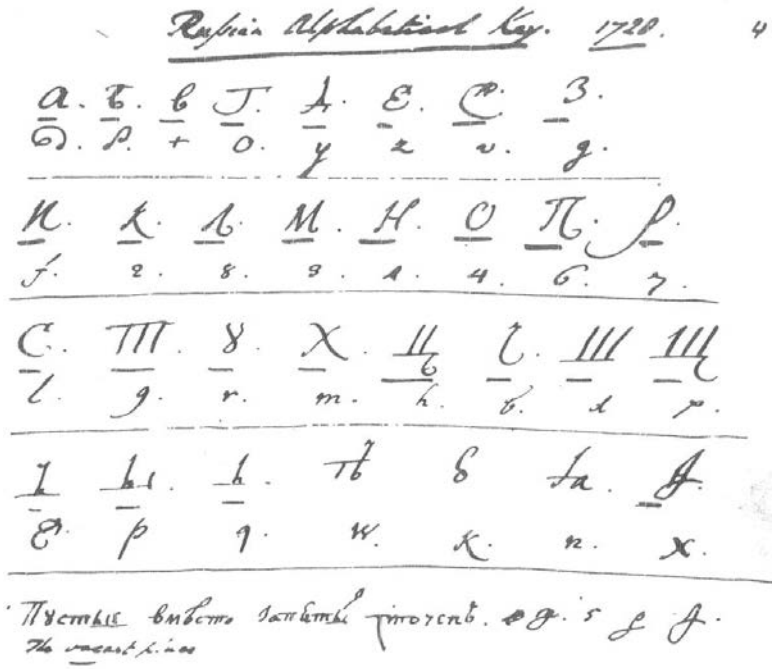
حل شفرات التبديل البسيطة

يعقوب بن إسحاق الكندي (801–873)

- طريقة (تحليل التكرار) معروفة منذ القرن التاسع.
- مخطوطة الكندي حول فك رموز رسائل التشفير.

متوسط تكرار الحروف في الإنجليزية





Russian monalphabetic key, recovered by England's Decyphering Branch, 1728

- مفتاح استبدال الحرف الروسي الأحادي، حيث تم استعادته (فك رموزه) من قبل فرع فك الرموز في إنجلترا في سنة 1728.
- مأخوذة من كتاب (*The Code Breakers*) لديفيد كان (David Kahn).

حكمة اليوم الثانية

- على مر التاريخ، استمر الناس في استخدام أساليب تشفير غير آمنة ولمدة طويلة حتى بعد ان تم كشف أساليب التشفير هذه، ربما بسبب الجهل والكسل أو غلبة الطبع.
- اليوم أيضًا، يستخدم الأشخاص تشفيرا غير آمن (أو بدون تشفير على الإطلاق)، حيث تقوم العديد من شركات التكنولوجيا بتسويق منتجات للتشفير تستخدم طرقًا غير آمنة تماما أو مزيفة.

شفرة الفيجينير(Vigenère Encryption)

- حيث يتم فيها استخدام عدة استبدالات لشيفرة القيصر وعمل دورة من خلالهم.
- سلسلة الاستبدالات يتم تحديدها عبر مفتاح سري.

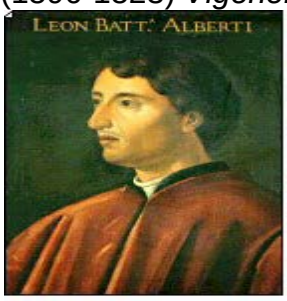

TRAICTE'
DES CHIFFRES,
OV SECRETES
MANIERES
D'ESCRIRE,
PAR
BLAISE DE VIGENERE,
BOVRBONNOIS.

A PARIS,

M. D. LXXXVII.

AVEC PRIVILEGE DV ROY.

بليز دي فيجينير *Blaise de Vigenere* (1596-1523).



ليون باتيستا ألبيرتي

Leon Battista Alberti

(1472-1404)

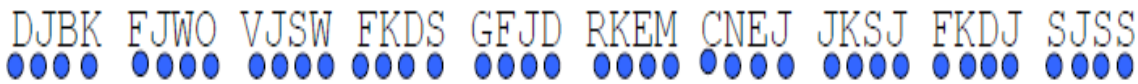
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
➡	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
➡	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
➡	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
➡	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
➡	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
➡	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
➡	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fight fiercely, Harvard! Fight! Fight! Fight!

XWTNU NZ H JQRR ZPRU NOEJ GQXK LTVM IBWL YVG

فك شيفرة الفيجينير(Vigenère)

- إذا كان المفتاح بطول K، فانه يتم عندئذٍ تحديد موضع حواشي النص المشفر K بواسطة نفس الحرف في المفتاح ...
- وهكذا تكون نتيجة استبدال بسيط،
- وبالتالي يمكن فك هذه الشيفرة بواسطة تحليل التكرار.
- مثال: لنفترض طول المفتاح هو ثلاثة:



لذا فإن فك التشفير يقلل إجراء تحليل التكرار بعدد K – **شريطة معرفة K**

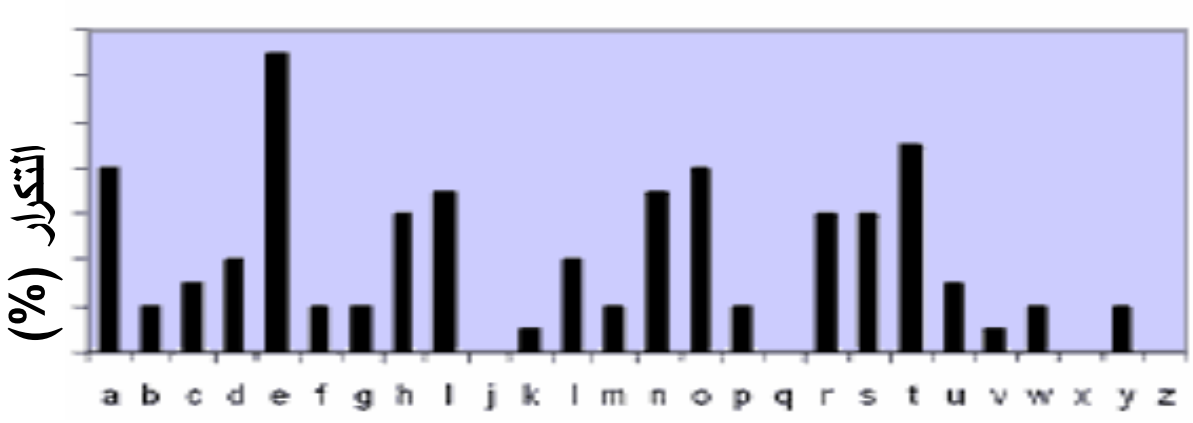
- للعثور على طول المفتاح:
- جرب قيمًا مختلفة لـ K، وذلك بالنظر إلى كل ظهورات حرف (K) في النص المشفر، واختيار الحرف التي يبدو فيها توزيع التكرار مثل توزيع التكرار في اللغة الإنجليزية.
- أساليب ذكية للقيام بذلك يدويا:

– باباج (Babbage) وكاسيسكي (Kasiski): القيام بعد الأحرف المزدوجة (خمسينيات وستينيات القرن قبل الماضي).

– فريدمان (Friedman): فهرس المصادفات (Index of Coincidence) في عشرينيات القرن الماضي.

- مع أجهزة الحاسوب، لا نحتاج إلى أن نكون أذكياء: فيمكننا القيام بإحصاءات هجوم التخمين (Brute-Force).

متوسط تكرار الحروف في الإنجليزية



لكن لنفترض أن المفتاح بطول الرسالة؟

- سوف تنهار طريقة فك التشفير،
- والمفتاح الذي يكون بطول الرسالة يدعى لوحة المرّة الواحدة (a one-time pad)
- يمكن اعتبار تشفير لوحة المرّة الواحدة هو تشفير آمن تمامًا، شريطة أن:
  - تكون اللوحة عشوائية،
  - يتم استخدام اللوحة **مرة واحدة فقط**.

كلود شانون (Claude Shannon 1916-2001)

النظرية الرياضية في الاتصال (A Mathematical Theory of Communication 1948)

Reprinted with corrections from *The Bell System Technical Journal*,
Vol. 27, pp. 379–423, 623–656, July, October, 1948.

A Mathematical Theory of Communication

By C. E. SHANNON

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one *selected from a set* of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design.

If the number of messages in the set is finite then this number or any monotonic function of this number can be regarded as a measure of the information produced when one message is chosen from the set, all choices being equally likely. As was pointed out by Hartley the most natural choice is the logarithmic function. Although this definition must be generalized considerably when we consider the influence of the statistics of the message and when we have a continuous range of messages, we will in all cases use an essentially logarithmic measure.

The logarithmic measure is more convenient for various reasons:

1. It is practically more useful. Parameters of engineering importance such as time, bandwidth, number of relays, etc., tend to vary linearly with the logarithm of the number of possibilities. For example, adding one relay to a group doubles the number of possible states of the relays. It adds 1 to the base 2 logarithm of this number. Doubling the time roughly squares the number of possible messages, or doubles the logarithm, etc.

2. It is nearer to our intuitive feeling as to the proper measure. This is closely related to (1) since we intuitively measures entities by linear comparison with common standards. One feels, for example, that two punched cards should have twice the capacity of one for information storage, and two identical channels twice the capacity of one for transmitting information.

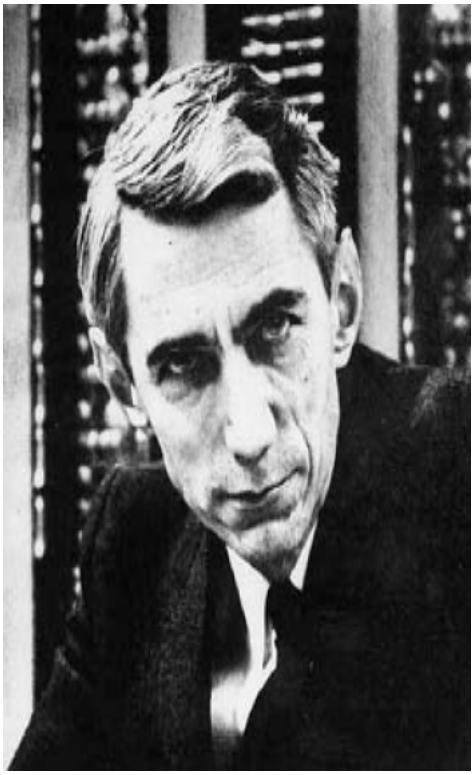
3. It is mathematically more suitable. Many of the limiting operations are simple in terms of the logarithm but would require clumsy restatement in terms of the number of possibilities.

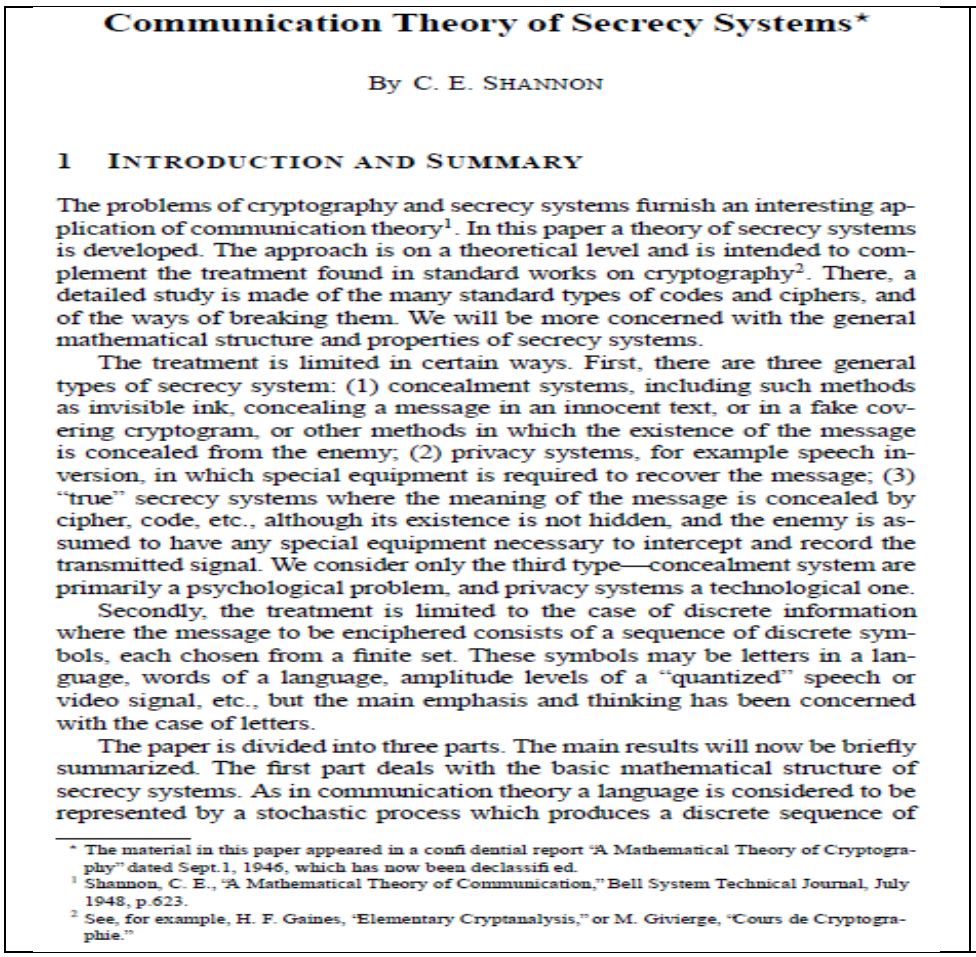
The choice of a logarithmic base corresponds to the choice of a unit for measuring information. If the base 2 is used the resulting units may be called binary digits, or more briefly *bits*, a word suggested by J. W. Tukey. A device with two stable positions, such as a relay or a flip-flop circuit, can store one bit of information. N such devices can store N bits, since the total number of possible states is 2^N and $\log_2 2^N = N$. If the base 10 is used the units may be called decimal digits. Since

$$\begin{aligned}\log_2 M &= \log_{10} M / \log_{10} 2 \\ &= 3.32 \log_{10} M,\end{aligned}$$

[1]Nyquist, H., "Certain Factors Affecting Telegraph Speed," *Bell System Technical Journal*, April 1924, p. 324; "Certain Topics in Telegraph Transmission Theory," *A.I.E.E. Trans.*, v. 47, April 1928, p. 617.
[2]Hartley, R. V. L., "Transmission of Information," *Bell System Technical Journal*, July 1928, p. 535.

1





Communication Theory of Secrecy Systems*

By C. E. SHANNON

1 INTRODUCTION AND SUMMARY

The problems of cryptography and secrecy systems furnish an interesting application of communication theory[1]. In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography[2]. There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general types of secrecy system: (1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy; (2) privacy systems, for example speech inversion, in which special equipment is required to recover the message; (3) "true" secrecy systems where the meaning of the message is concealed by cipher, code, etc., although its existence is not hidden, and the enemy is assumed to have any special equipment necessary to intercept and record the transmitted signal. We consider only the third type—concealment system are primarily a psychological problem, and privacy systems a technological one.

Secondly, the treatment is limited to the case of discrete information where the message to be enciphered consists of a sequence of discrete symbols, each chosen from a finite set. These symbols may be letters in a language, words of a language, amplitude levels of a "quantized" speech or video signal, etc., but the main emphasis and thinking has been concerned with the case of letters.

The paper is divided into three parts. The main results will now be briefly summarized. The first part deals with the basic mathematical structure of secrecy systems. As in communication theory a language is considered to be represented by a stochastic process which produces a discrete sequence of

* The material in this paper appeared in a confidential report "A Mathematical Theory of Cryptography" dated Sept. 1, 1946, which has now been declassified.

[1] Shannon, C. E., "A Mathematical Theory of Communication," Bell System Technical Journal, July 1948, p. 623.

[2] See, for example, H. F. Gaines, "Elementary Cryptanalysis," or M. Givierge, "Cours de Cryptographie."

- شانون: "نظرية الاتصالات للأنظمة السرية"، 1949
- على أساس العمل المصنف الذي أنجز في عام 1946

"السرية التامة" (شانون، 1949)

- التعريف: يتمتع نظام التشفير بسرية تامة إذا كانت معرفة النص المشفر لا تخبرك بأي معلومات عن النص الصريح.
- النتيجة 1: من أجل الحصول على سرية تامة، يجب أن يكون المفتاح بطول الرسالة.
- النتيجة 2: يمكن أن يكون نظام لوحة المرّة الواحدة سري تماما إذا تم استخدامه لمره واحده فقط.

التشفير مع الحواسيب

- تريد تشفير وحدات البت bits (مثل النص، والموسيقى، والصور، ...)، وليس مجرد تشفر الأحرف.
- بدلاً من تحريك الحروف مسافة ما، استخدم عمليات البت مثل بوابة الاختيار الحصري أو بوابة اكس اور (XOR)، {من المترجم: وهي بوابة منطقية متعددة المداخل ولها مخرج واحد}...

بوابة الاختيار الحصري Exclusive OR (XOR), a⊕b

- التعريف: لدينا 2 من البتات (bits): ةهما a و b
  - a⊕b = 0 إذا كانت قيمة a وقيمة b هي نفسها (كلاهما 0 أو كلاهما 1)،
  - a⊕b = 1 إذا كانت قيم a و b مختلفة.

• الجمع بين بيانات البتات (Data Bitwise)، وذلك باستخدام XOR
• مثال:

$$01000010 \oplus 01010011 = 00010001$$

تشفير XOR (البتات التناظرية من فيجنير Bit analog of Vigènere)

المفتاح	SECRET
الرسالة الصريحة	Bill Gates's SSN is 539-60-5125
المفتاح مكرر	SECRETSECRETSECRETSECRETSECRETSE

الرسالة في اسكي كود (ASCII)

b	i	1	1	.....	5
01000010	01101001	01101100	01101100	.....	00110101

Repeated key in ASCII المفتاح مكرر في اسكي كود

S	E	C	R	.....	R
01010011	01000101	01000011	01010010	.....	01000101

Bit-wise xor

00010001	00101100	00101111	00111110	.....	01110000

أساليب التشفير في الحاضر

- أساليب غير آمنة للتشفير:

  – يوجد الكثير من الأساليب غير الآمنة للتشفير في جميع أنحاء:
    - من الهواة،
    - والشركات "الأمنية" المبتدئة،
    - وكذلك من الشركات الناشئة.

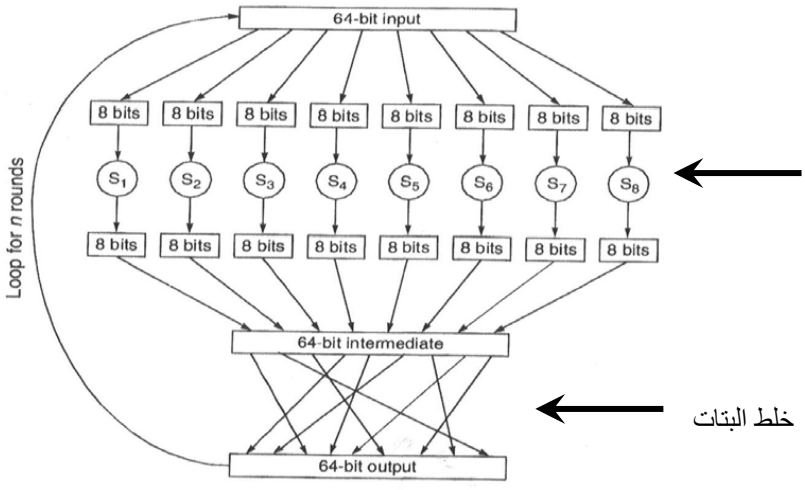
- أساليب آمنة للتشفير:

  – أسلوب لوحة المرة الواحدة هي الطريقة الوحيدة الآمنة،
    - ولكن هذا يتطلب نقل هذه اللوحة بشكل آمن.
  – العديد من الخوارزميات الأخرى التي صمدت لسنوات من التحليل ومحاولات الهجوم.

معيار تشفير البيانات (DES)

- صمم هذا المعيار من شركة أي.بي.أم (IBM) في عام 1975، بمساعدة من وكالة الأمن القومي الأمريكي (NSA):

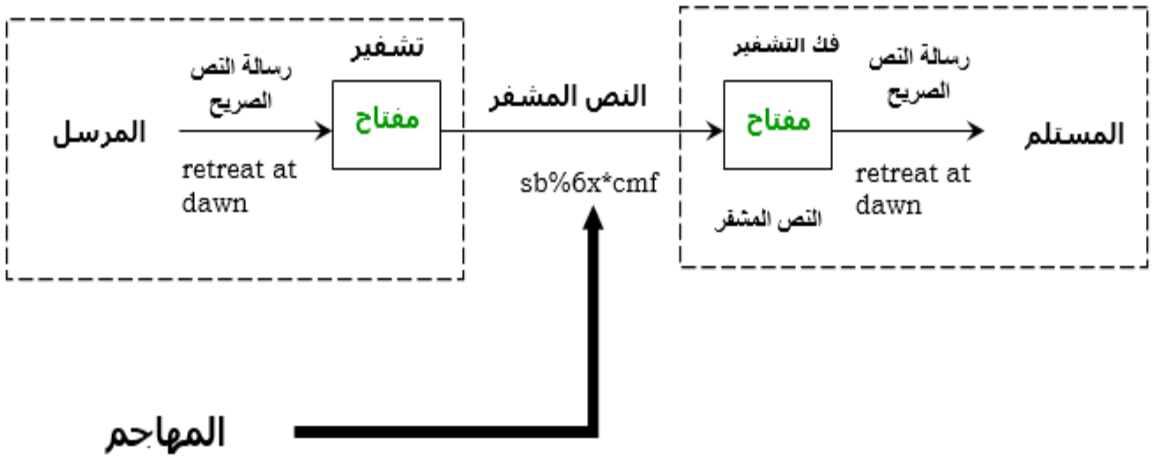
–يقوم بتشفير وحدات 64 بت، على أساس مفتاح 56 بت.



سرية معيار تشفير البيانات (Security of DES)

- **لا اختصارات، بقدر ما يعرف الجميع:**
  - عليك أن تجرب كل المفاتيح الممكنة،
  - المفاتيح هي بطول 56 بت، لذلك سيكون هناك 2 أس 56 مفتاح (2^{56}).
  - 2^{56} هو عدد كبير، ولكن ليس بالهائل. ففي آب/أغسطس 1998، أثبتت مؤسسة الحدود الإلكترونية (Electronic Frontier Foundation) أن آلة ذات أغراض خاصة مبنية من أجزاء قياسية بتكلفة قدرها 200 ألف دولار يمكن أن تكسر DES في غضون 56 ساعة.
- **الحكومات الكبيرة لديها أكثر من 200 ألف دولار لإنفاقها على تحليل الشفرات.**
- **في كل مرة تضيف فيها بت إلى طول المفتاح، يتضاعف الوقت اللازم لكسر النظام.**
- **اعتمد المعهد الوطني للمعايير والتقنية (NIST) معيار التشفير المتقدم الجديد في عام 2001**
- **(خوارزمية Rijndael، من مفاتيح 128 بت). ولا زال DES يستخدم على نطاق واسع.**

نظم التشفير (Cryptosystems)



بعض أنواع الهجمات:

- **النص المشفر فقط،**
- **نص صريح معروف،**
- **نص صريح مختار،**
- **نص مشفر مختار،**
- **خرطوم مطاطي** (Rubber Hose) ... {من المترجم: الخرطوم المطاطي تعني تحصيل كلمات السر أو مفتاح التشفير من المستعمل بالقوة).

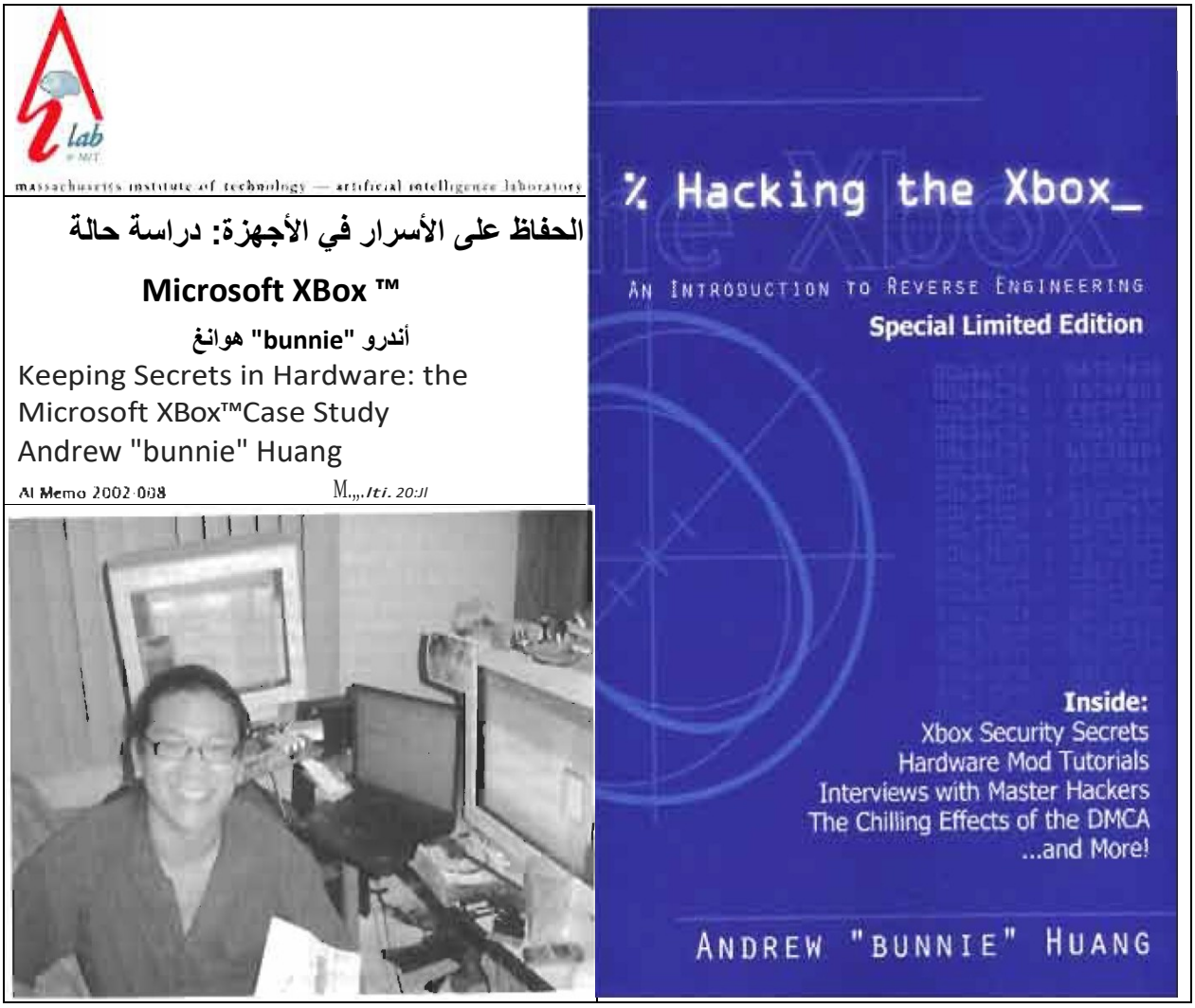
مبدأ كيركوف (Kerckhoffs Principle)

- **أوغست كيركوف (Auguste Kerkhoffs)، من المصدر: التشفير العسكري (La Cryptographie Militaire)، 1883.**
- **يجب تصميم أنظمة التشفير بطريقة لا تتأثر إذا كان الخصم يتعرف على التقنية المستخدمة. بعبارة أخرى، يجب أن يتواجد الأمن في اختيار مفتاح التصميم بدلاً من ميزات التصميم الغامضة. {من المترجم:** أن **رسالتك السرية** يجب أن تعتمد على **سرية مفتاح التشفير** وليس على **سرية نظام التشفير}.**

– من المصدر: روس أندرسون (Ross Anderson) "كيف تغش في اليانصيب" (1999).

اقتباس من شناير(Schneier)

- **إذا كانت قوة نظام التشفير الجديد الخاص بك يعتمد على حقيقة أن المهاجم لا يعرف العمل الداخلي للخوارزمية، فانت في ورطة. وإذا كنت تعتقد أن الحفاظ على سرية الخوارزميات يحسن أمن نظام التشفير الخاص بك أكثر من السماح للمجتمع الأكاديمي بتحليله، فأنت مخطئ. وإذا كنت تعتقد أن شخصًا ما لن يفك شفرة الكود ولن يعيد هندسة الخوارزمية الخاصة بك، فستكون ساذجًا.**
- **بروس شناير (Bruce Schneier) من كتاب تطبيق التشفير (Applied Cryptography). (طبعة 2، 1996).**


lab
massachusetts institute of technology — artificial intelligence laboratory
الحفاظ على الأسرار في الأجهزة: دراسة حالة
Microsoft XBox ™
أندرو "bunnie" هوانغ
Keeping Secrets in Hardware: the Microsoft XBox™Case Study
Andrew "bunnie" Huang
AI Memo 2002-008
% Hacking the Xbox_
An Introduction to Reverse Engineering
Special Limited Edition
Inside:
Xbox Security Secrets
Hardware Mod Tutorials
Interviews with Master Hackers
The Chilling Effects of the DMCA
...and More!
Andrew "bunnie" Huang

نهاية الجزء الأول

استمرار ...

لا شيء من هذا مناسب لتطبيقات الإنترنت

- **من أجل التواصل، يجب على أليس وبوب مشاركة المفتاح السري:**
  - لا يعمل هذا الأمر بشكل جيد على النطاق الواسع،
  - لا يعمل هذا الأمر مع الأطراف التي لم تقم بإجراء ترتيب آمن بشكل مسبق.
- **ولكن هناك فكرة رائعة:**
- **يمكن لأليس وبوب إنشاء مفتاح سري مشترك، حتى لو لم يلتقيا من قبل ولم يقوما بترتيبات مسبقة، وحتى إذا كان بإمكان الجميع التنصت على جميع اتصالاتهم ...**
- **... بما في ذلك التنصت على الاتصالات التي يستخدمونها لإنشاء المفتاح!**

تشفير المفتاح العام

تمت إزالة الصور بسبب حقوق الطبع والنشر من المصدر.

الفكرة الأساسية لتبادل مفتاح ديفي–هيلمان–ميركل

The basic idea of Diffie–Hellman–Merkle key agreement

- **ترتيب الأشياء بحيث:**
  - أليس تحسب رقمًا استنادًا إلى معلومات سرية والتي **لا يعرفها أحد سوى أليس فقط،**
  - بوب يحسب رقمًا استنادًا إلى معلومات سرية والتي **لا يعرفها أحد سوى إلا بوب فقط،**
  - أليس وبوب سوف يرتبان بطريقة ما عملية احتساب **الرقم نفسه،** على الرغم من عدم معرفتهما للمعلومات السرية لبعضهما البعض،
  - لا يمكن لأي شخص آخر احتساب هذا الرقم بدون معرفة معلومات أليس السرية أو معلومات بوب السرية.
- **قد يبدو ان هذا الأمر مستحيلا...**

اختبار رياضي

mod هي باقي القسمة الصحيحة:

$$2 \times 6 = 1 \mod 11$$

$$2 \times 6 \times 5 = 5 \mod 11$$

$$2^3 = 1 \mod 7$$

$$2^{300} = 1 \mod 7$$

هناك اختصار لاحتساب القوة (الأس)

- المسألة: إذا أعطيت a و p و x ، فقم بإيجاد y بحيث:

$$a^x = y \pmod p$$

- الطريقة 1: ضرب a في نفسه x مرة
  - يتطلب عمليات ضرب x
- الطريقة 2: استخدام التربيعات المتعاقبة (successive squaring)
  - يتطلب عمليات ضرب Lg x
- تعمل نفس الفكرة من أجل صيغة الضرب p
- مثال: إذا كان x رقمًا مكونًا من 500 منزلة، فيمكننا حسابه بعدد خطوات:

$$a^x \pmod p \text{ in about } 1700 \ (= \lg 10^{500})$$

لا يوجد اختصار لاحتساب باقي القسمة الصحيحة للوغاريتمات

- المشكلة: إذا أعطيت a و p و y ، فقم بإيجاد x بحيث:

$$a^x = y \pmod p$$

- نعلم جميعا انه لا توجد طرق مختصرة.
  - الطريقة الوحيدة للقيام بذلك هي في الأساس عن طريق البحث باستخدام هجوم التخمين (Brute-Force) بين جميع احتمالات x
- مثال: إذا كان p رقمًا من 500 منزلة، فإن العثور على x يتمثل بالآتي

$$a^x = y \pmod p$$

وتتطلب حوالي 10^{500} خطوة.

العملية الرياضية لتبادل مفتاح ديفي–هيلمان–ميركل

The math behind DHM key agreement

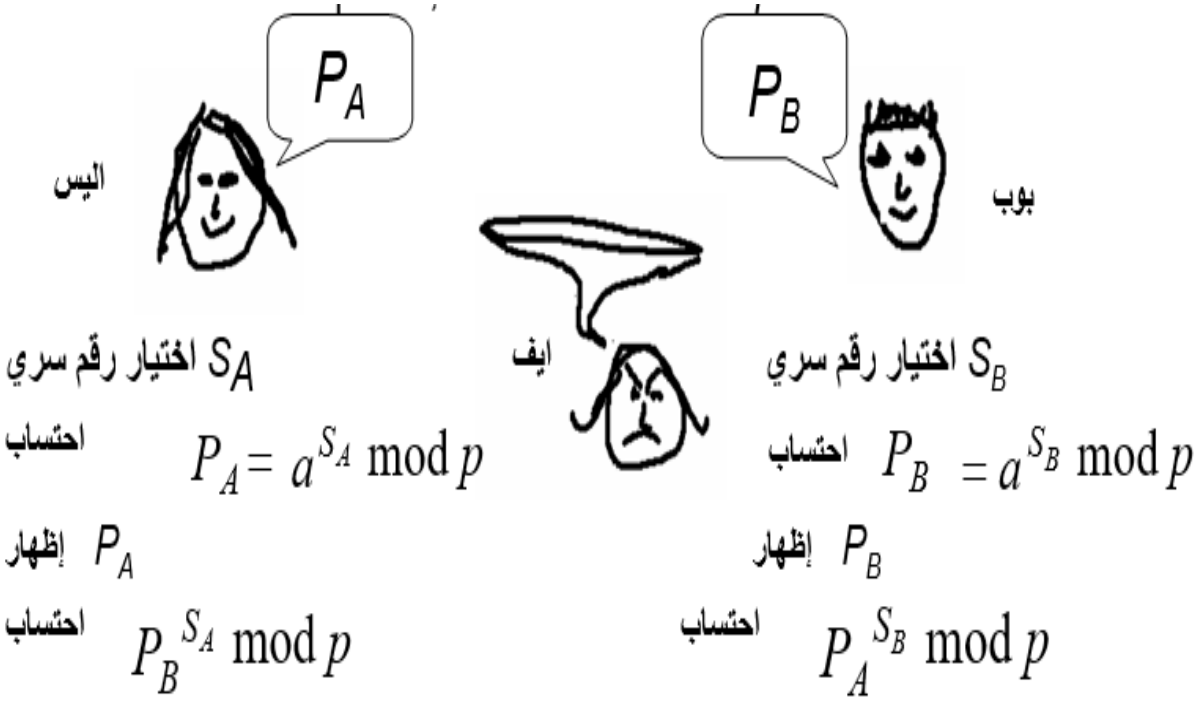
- **إذا أعطيت a و p ، ومعادلة من النموذج**

$$a^x = y \pmod{p}$$

- **ومن ثم فان حساب x إذا أعطيت y يعتبر أكثر صعوبة من حساب y إذا أعطيت x.**
- **أما بالنسبة للأرقام المكونة من 500 منزلة، فاننا نتحدث عن جهد لحساب يبلغ 1700 خطوة مقابل 10^{500} خطوة.**

تبادل مفتاح ديفي–هيلمان–ميركل

ابدأ بالقيم العامة والقياسية لـ p و a



النقطة الرئيسية: لقد حسبت أليس وحسب بوب نفس العدد، لأن:

$$\left(P_B{}^{S_A} = (a^{S_B})^{S_A} = a^{S_B S_A} = (a^{S_A})^{S_B} = P_A{}^{S_B}\right) \bmod p$$

يمكن الآن لأليس وبوب استخدام هذا الرقم كمفتاح مشترك للاتصالات المشفرة

فالمتصنت يعرف ان:

$$P_A = a^{S_A} \bmod p \quad \text{and} \quad P_B = a^{S_B} \bmod p$$

لكن الذهاب من هذه المعادلة إلى حسبة:

$$a^{S_A S_B} \bmod p$$

يتطلب احتساب لوغاريتمات mod p، كما هو معروف للجميع.

بريد إلكتروني سري مع

"ديفي–هيلمان–ميركل بدون اتصال"


أليس

تقوم أليس باختيار المفتاح السري S_A، وتحسب المفتاح العام المقابل P_A (باستخدام صيغة D-H) وتنشر P_A في دليل.

لإرسال رسالة أليس،


بوب

– بوب يقوم بالبحث عن المفتاح العام لأليس، واختيار رقم عشوائي للقيام بدور S_B لهذه الرسالة، وحساب P_B المقابل (باستخدام صيغة D-H).

– ويقوم بوب باستخدام S_B ومفتاح أليس العمومي لإنشاء مفتاح تشفير لهذه الرسالة (باستخدام صيغة D-H).

– ويقوم بوب بإرسال الرسالة المشفرة إلى أليس مع P_B.


أليس

تستخدم أليس مفتاحها السري وتستخدم P_B التي تلقتها من بوب للقيام بحساب المفتاح وفك تشفير الرسالة.

لكن هناك مشكلة

- كيف يمكن لبوب أن يعرف أن القائمة في الدليل هي في الحقيقة المفتاح السري لأليس؟


أليس

تقوم أليس باختيار المفتاح السري S_A، وتحسب المفتاح العام المقابل P_A وتنشر P_A في دليل،


أيف

تعبث في الدليل وتدخل مفتاحها الخاص تحت اسم أليس


بوب

يقوم بغير وعي باستخدام المفتاح العام لـ "أليس" من الدليل، ولكنه في الواقع يرسل رسائل يمكن لـ أيف ان تفك تشفيرها.

خوارزميات التوقيع الرقمي

- إذا تم الحصول على المفتاح السري، فان المفتاح العمومي المقابل مع الرسالة تولد رقم SIG مثل الآتي:
  - من السهل حساب SIG إذا كنت تعرف المفتاح السري والرسالة،
  - SIG غير قابل للحساب إذا لم تكن تعرف المفتاح السري،
  - من السهل "التحقق" من قبل أي شخص يعرف الرسالة والمفتاح العام. أي يجب أن يكون الشرط المعين المضمن بالرسالة و SIG والمفتاح العمومي صالحًا.
- خوارزميات التوقيع الرقمي تشبه إلى حد كبير خوارزمية ديفي–هيلمان–ميركل.
- تعتبر نظام ريفست–شامير–أدلمان (RSA: Rivest–Shamir–Adleman) هي أول نظام عملي للقيام بالتواقيع الرقمية، كما قام أيضًا بتشفير المفاتيح العمومية.
- لتوقيع رسالة، فعليك القيام بحساب SIG باستخدام مفتاحك السري. ويمكن لأي شخص التحقق من SIG باستخدام مفتاحك العام.
- إذا تم العبث بالرسالة، فان التوقيع لن يتحقق. [النزاهة].
- لا أحد غيرك يمكنه إنتاج SIG، لأن إنتاج SIG يتطلب معرفة مفتاحك السري. [المصادقة وعدم التنصل]

الشهادات والهيئات التي تصدر الشهادات *
البنى التحتية للمفتاح العام (PKI)

- **كيف نعرف أن "مفتاح أليس العام" ينتمي في الواقع إلى أليس؟**

– **تذهب أليس إلى إحدى هيئات إصدار الشهادات (CA) وتوضح هويتها وتعرض مفتاحها العام، فتقوم الهيئة (CA) بالتوقيع الرقمي لمفتاح أليس العام، وإنتاج الشهادة، وبالتالي ويمكن لأي شخص التحقق من صلاحية الشهادة باستخدام المفتاح العام للهيئة.**

- **كيف نعرف أن مفتاح الهيئة العمومي (CA) هو في الواقع له؟**

– **1. لدى الهيئة العمومية (CA) أيضاً شهادة موقعة من قبل بعض الهيئات المعروفة والموثوقة مثل مكتب البريد الأمريكي (سلسلة الثقة)؛ و / أو**

– **2. الكثير من الناس الذين نثق بهم قد قاموا بالمصادقة عليه من خدمة (Web of trust)**

* لورين كونفيلدر. (Loren M Kohnfelder) نحو نظام تشفير عملي للمفتاح العام. أطروحة البكالوريوس، قسم EECS، معهد ماساتشوستس للتكنولوجيا. مايو، 1978.

بروتوكول أمن طبقة النقل الأساسية

(Basic Transport Layer Security Protocol)

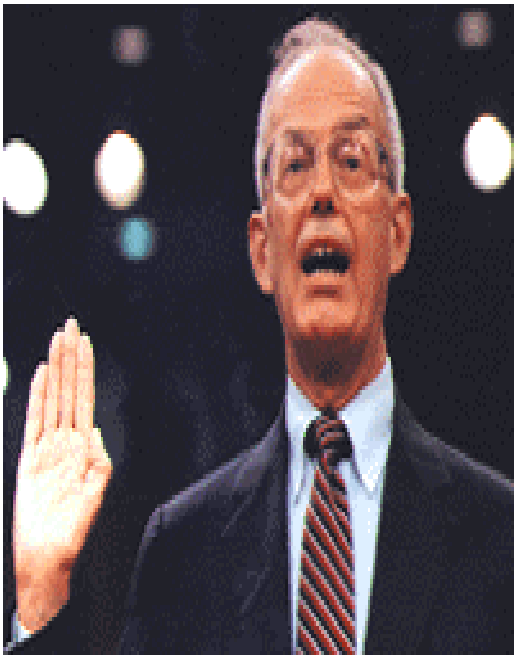
(الاسم القديم SSL)

نهاية الجزء الثاني

استمرار ...

National Security Agency

وكالة الأمن القومي



هناك خطر حقيقي وجدي للغاية يتمثل في أن النقاش العام غير المقيد لمسائل عِلْمُ الاتِّصالاتِ السِّرِّيَّة (Cryptologic) سيضر بشكل خطير بقدرة الحكومة على إجراء معلومات استخباراتية وقدرة الحكومة على القيام بمهمتها في حماية معلومات الأمن القومي من الاستغلال العدائي.

-الأدميرال بوبي راي إنمان (Bobby Ray Inman)

(مدير وكالة الأمن القومي، 1979).

ما لم يتم حل مسألة التشفير قريبًا، ستصبح المحادثات الجنائية عبر الهاتف وأجهزة الاتصالات الأخرى غير مفهومة من جانب سلطات إنفاذ القانون.

هذا الأمر مثل أي قضية، تهدد السلامة العامة والأمن القومي في البلد. وعصابات المخدرات والإرهابيون والخاطفون سوف يستخدمون الهواتف ووسائل الإعلام الأخرى مع إفلاتهم من العقاب وهم يعلمون أن محادثاتهم محصنة ضد أفضل أساليبنا في التحقيق.

مدير مكتب التحقيقات الفيدرالي لويس فريه، شهادة في الكونغرس 30 مارس، 1995.

CALEA، تشرين الأول 1994

{من المترجم: CALEA هو قانون سن في الكونجرس لمساعدة الاتصالات من أجل فرض القانون}:

... يجب على شركة الاتصالات السلكية واللاسلكية ... أن تضمن أن معداتها أو مرافقها أو خدماتها ... قادرة على ... فرز فعال وتمكين للحكومة، بموجب أمر قضائي أو تفويض قانوني آخر، من اعتراض... جميع الاتصالات السلكية والإلكترونية التي يحملها الناقل في منطقة خدمة من أو إلى معدات أو مرافق أو خدمات مشترك في هذه الشركة حالا مع نقلها إلى/ أو من معدات أو منشآت أو خدمات المشترك، أو في وقت لاحق اذا كان هذا مقبولاً للحكومة...

TOP SECRET

30007

THE WHITE HOUSE

WASHINGTON

January 17, 1991

MEMORANDUM FOR THE HONORABLE DICK CHENEY
Secretary of Defense

THE HONORABLE WILLIAM P. BARR
Attorney General

THE HONORABLE ROBERT M. GATES
Director of Central Intelligence

SUBJECT: Legislative Strategy for Digital Telephony (S)

On December 30, 1991, I sent to the President a memorandum seeking his approval for a legislative strategy for digital telephony. The substance of that memorandum is attached. On January 15, 1992, he approved the following course of action:

- Justice should go ahead now to seek a legislative fix to the digital telephony problem, and all parties should prepare to follow through on the encryption problem in about a year. Success with digital telephony will lock in one major objective; we will have a beachhead we can exploit for the encryption fix; and the encryption access options can be developed more thoroughly in the meantime. (TS)

Brent Scowcroft

Attachment

TOP SECRET
Declassify on: OADR

TOP SECRET

10

Telephony (S)

On December 30, 1991, I sent to the President a memorandum seeking his approval for a legislative strategy for digital telephony. The substance of that memorandum is attached. On January 15, 1992, he approved the following course of action:

- Justice should go ahead now to seek a legislative fix to the digital telephony problem, and all parties should prepare to follow through on the encryption problem in about a year. Success with digital telephony will lock in one major objective; we will have a beachhead we can exploit for the encryption fix; and the encryption access options can be developed more thoroughly in the meantime. (TS)

Brent Scowcroft

Attachment

TOP SECRET
Declassify on: OADR

TOP SECRET

10

شريحة كليبر (Clipper)

{من المترجم: شريحة أو رقاقة "كليبر" عبارة عن رقاقات تم تطويرها وترويجها من قبل وكالة الأمن القومي الأمريكية كجهاز تشفير يحمي الرسائل الصوتية والكتابية عبر وجود باب خلفي مدمج، وكان من المفترض أن تعتمده شركات الاتصالات لنقل الصوت، بحيث يمكن تشفير وفك تشفير الرسائل، وكانت جزءًا من برنامج إدارة كلينتون للسماح لمسؤولي تطبيق القانون الفيدراليين والمحليين باعتراض وفك تشفير البيانات الصوتية والمكتوبة}

- **صممت من قبل وكالة الأمن القومي (NSA): "للهواتف فقط".**
- **تم الإذن به بتعليمات سرية من كلينتون في أبريل 1993 (تم الإعلان أنهم كانوا يقومون بتقييمه فقط). والمعايير صدرت في فبراير 1994.**
- **اعتبر طوعيا (ولكن الحكومة ستشتري فقط هواتف كليبر).**
- **المفتاح المدمج ("الباب الخلفي") والذي قسم بحيث: كل نصف تحتفظ به وكالة حكومية مختلفة ("مؤتمن المفتاح Key Escrow").**
- **خوارزمية التشفير السرية: يجب أن تكون شرائح كليبر محصنة ضد العبث وبالتالي مكلفة.**
- **لا تعمل هواتف كليبر مع الهواتف التي لا تستخدم شريحة كليبر.**
- **رقاقة "كابستون" (Capstone) لبيانات لحاسوب والاتصالات.**

حروب مؤتمن المفتاح (Key Escrow)

- **شخصيات المسرحية (Dramatis Personae)، أي المعنيون بالقضية:**
  - **الصناعة،**
  - **إنفاذ القانون،**
  - **الأمن القومي،**
  - **مجموعات التحرر المدني.**

مطرقة الحكومة الكبيرة: ضوابط تصدير التشفير

- **قبل عام 1995: تكنولوجيا التشفير صنفت من قبل وزارة الخارجية كذخيرة (سلاح):**
  - تصدير الأجهزة والبرمجيات والمعلومات الفنية يعتبر غير قانوني، ما لم تسجل كتاجر أسلحة وتتقيد بالأنظمة الصارمة.
  - تقديم المساعدات المادية أو التقنية إلى الأفراد غير الأمريكيين يعتبر مخالفا للقانون، بما في ذلك النشر على الإنترنت حيث يكون ذلك متاحًا خارج الولايات المتحدة.
- **1995: بيرنشتاين (Bernstein) رفع دعوى قضائية ليطعن في دستورية لوائح التصدير ضد وزارة الخارجية الأمريكية وآخرون.**
- **1996: تم تحويل الولاية القضائية لصادرات التشفير إلى وزارة التجارة، ولكن القيود بقيت.**
- **1996–2001: عدلت قوانين التشفير وخففت، ولكنها بقيت موجودة (على سبيل المثال، لا يمكن تصديرها إلى قائمة من بعض الدول).**
- **2003: حتى هذا العام قضية بيرنشتاين (Bernstein) لا تزال في المحاكم.**

مطالبات وقضايا الصناعة (1995)

- الزبائن يريدون الأمن للتجارة الإلكترونية لأجل حماية الوصول عن بعد، ولسرية المعلومات التجارية.
- قيود التصدير هي مزعجة جدا.
- هناك طلب تجاري معقول لـ "الوصول الاستثنائي" إلى البيانات المشفرة المخزنة (على سبيل المثال، شخص فقد مفتاحًا ما للتشفير)؛ لكن طلب الوصول إلى الاتصالات المشفرة يعتبر ضعيفا، ولا يوجد أي طلب تجاري للوصول السري.

مطالبات ومسائل إنفاذ القانون (1995)

- التنصت على المكالمات هو أداة حاسمة لإنفاذ القانون.
- يتم إجراء التنصت على أهداف محددة وخاصة تحت سلطة قانونية.
- بالنسبة للتصنت يجب أن يتم الوصول إلى مفاتيح الضمان (Escrowed Keys) بدون معرفة أصحاب المفاتيح.
- كثير من المجرمين غالبًا ما يكون مهملين و / أو أغبياء: فهم لن يستخدموا التشفير إلا إذا أصبح شائعا. وبعض المجرمين بعيدون كل البعد عن الغباء أو الإهمال: وسوف يستخدمون التشفير إذا كان متاحًا.
- الأدلة التي تم الحصول عليها من فك التشفير يجب أن تصمد أمام المحكمة.
- هناك حاجة للتعاون الدولي في مجال إنفاذ القانون.

مطالبات وقضايا مؤسسة الأمن القومي (1995)

- **لا يمكننا إخبارك، لكنهم جادون حقًا.**
- **وكالة الأمن القومي (NSA) يشاع أنها "تنفذ" اعتراضات شاملة للاتصالات على نطاق واسع، باستخدام أجهزة الحاسوب لتصفية حركة المرور المثيرة للاهتمام.**

البرلمان الأوروبي

EUROPEAN PARLIAMENT

1999		*2004*

وثيقة الجلسة

11 يوليو 2001

التقرير الأخير

وجود نظام عالمي لاعتراض الاتصالات الخاصة والتجارية (نظام اعتراض ECHELON).

مطالبات وقضايا الحرية المدنية (1995)

- **مع ازدياد واتساع تكنولوجيا الاتصالات الحاسوبية، يصبح السماح للحكومة بالوصول إلى الاتصالات قضية أكثر بكثير من التنصت التقليدي على المحادثات الهاتفية.**
- **كيف يتم حمايتنا من إساءة استخدام النظام؟**
- **إذا سهلنا عملية التنصت، فما هو التحقق على استخدامها المتزايد؟**
- **هناك أدوات أخرى (التنصت، استخراج البيانات، مطابقة الحمض النووي) التي يمكن أن تساعد في إنفاذ القانون. فالناس لديها خصوصية أقل من ذي قبل حتى بدون التنصت.**

اجتماعات المعهد القومي الأمريكي للمعايير والتقانة (NIST) مع الصناعة، خريف 95

- **السماح بتصدير الأجهزة والبرمجيات باستخدام خوارزميات تصل إلى 56 بت، شريطة أن يتم تسليم مفاتيح الائتمان لـ "وكلاء ائتمان" (Escrow Agents) معتمدين من الحكومة.**
- **لكن:**

– عدم قابلية العمل المشترك بين الأنظمة المضمونة (التي لها مفاتيح الائتمان) والأنظمة غير المضمونة.

– لا يمكن تعطيل الائتمان.

– يجب أن يكون وكلاء الائتمان (Escrow Agents) مصدقين من قبل حكومة الولايات المتحدة أو الحكومات الأجنبية التي لدى الولايات المتحدة اتفاقيات رسمية معها.

- **المحادثات انهارت.**

مسودة مجموعة العمل المشتركة بين الوكالات، مايو 96

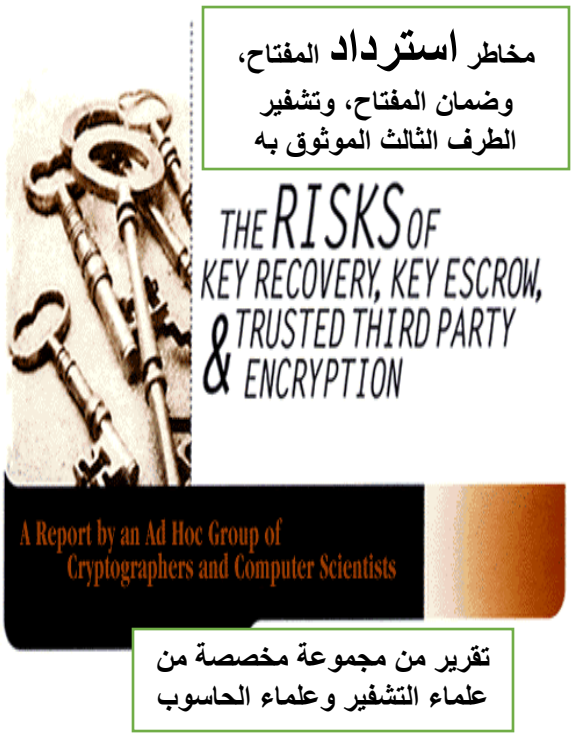
- يجب على شركات الصناعة والحكومة المشاركة في تطوير بنية تحتية أساسية لإدارة المفاتيح العامة والمنتجات المصاحبة التي تضمن أن المشاركين يستطيعون إرسال المعلومات وتلقيها إلكترونياً بثقة في سلامة المعلومات وأصالتها وأصلها والتي تضمن الوصول القانوني في الوقت المناسب للحكومة.
- الضمان هو ثمن الشهادة (قد يكون هيئات إصدار الشهادات CA أيضا بمثابة وكلاء تأمين المفتاح EA).

مغازلة الصناعة، خريف 96 ...

- نقل الاختصاص في صادرات التشفير من الدولة إلى التجارة.
- السماح بتصدير أي قوة، طالما أنها تحتوي على مؤتمن المفتاح (المعروف الآن باسم "استرداد المفتاح" KR).
- الموافقة الفورية على التصدير للمنتجات الملتزمة ب 56 بت على معيار تشفير البيانات (DES)، اذا ما قدمت ملفات الشركة خطة لتثبيت KR في المنتجات الجديدة 56 في غضون عامين.
- زيادة منح تراخيص التصدير للتطبيقات المقيدة (مثل المعاملات المالية).

التشريع، 1997

- **مشاريع القوانين المقدمة في جميع المواضيع، بدءا من إلغاء ضوابط التصدير إلى مشاريع القوانين التي من شأنها أن تكفل استرداد المفتاح للاستخدام المنزلي.**



- Hal Abelson
- Ross Anderson
- Steven M. Bellovin
- Josh Benaloh
- Matt Blaze
- Whitfield Diffie
- John Gilmore
- Peter G. Neumann
- Ronald L. Rivest
- Jeffrey I. Schiller
- Bruce Schneier

بعض الملاحظات الفنية

- إذا تمكنت أليس وبوب من المصادقة على بعضهما البعض، فيمكنهما استخدام ديفي-هيلمان (Diffie-Hellman) لإنشاء مفتاح مشترك للاتصالات.
- تختلف المتطلبات الأمنية لهيئات إصدار الشهادات (CA) عن متطلبات وكلاء ائتمان المفتاح.
- تطبيق التشفير الأساسي يعتبر غير مكلف، ولكن إضافة بنية تحتية لاسترداد المفتاح مكلف.
- التشفير ضروري ليس فقط للتجارة الإلكترونية، بل لحماية البنية التحتية للمعلومات. ولكن ائتمان المفتاح قد يجعل الأمور أقل أمانًا، وليس أكثر من الاتي:
  - يمكن أن تكون مستودعات المفاتيح المؤتمنة أو المودعة أهدافًا لا تقاوم للهجوم من قبل المجرمين.
  - إذا كان بإمكان الآلاف من الموظفين المكلفين بتنفيذ القانون الوصول بسرعة إلى المفاتيح المستحقة، فحينئذٍ يوجد تسأل: من يستطيع أيضا الوصول إلى تلك المفاتيح؟

في الآونة الأخيرة...

- يناير، 2000: وزارة التجارة تصدر لوائح تصديرية جديدة حول التشفير وقيود مخففة.
- 13 سبتمبر 2001: السناتور جود جريج Judd Gregg (نيو هامبشاير) يدعو إلى وجود لوائح للتشفير ، قائلاً إن صانعي التشفير "معرضون للخطر على نحو كبير كما لو كنا معرضين للخطر كأمة، ويجب أن يفهموا أنهم كمواطنين، لديهم التزام" لكي تشمل الوكالات الحكومية في أساليب فك التشفير.
- بحلول شهر أكتوبر، غيّر جريج رأيه حول إدخال التشريعات.
- سؤال: لماذا كان عام 2001 مختلفًا تمامًا عن عام 1997؟

VoIP Blog - VoIP News, Gadgets

VoIP & Gadget News Blog with the latest news in the VoIP and gadget space, smart phones, product reviews, opinion & analysis.

Home | Archives | VoIP Forums | About | Contact

« Skype v1.4 Released (soon) | Main | JiWire WiFi toolbar »

FCC requires some broadband and VoIP Providers to accommodate wiretaps

September 28, 2005

I must have missed the FCC's announcement 3 days ago that the FCC was going to require certain broadband and VoIP Providers to accommodate wiretaps. The 59-page FCC report is a bit lengthy for me to digest today, so maybe I'll provide a more detailed analysis tomorrow.

A quick speed read seems to indicate the FCC is going to force Internet providers to accomodate wiretaps, but that *doesn't include cafes or hotels that use or pay for Internet service*. I guess the FCC is targetting the main ISPs and not resellers of Internet service. Here's a very interesting excerpt that sums up **who is** covered by CALEA wire-tapping rules:

> We conclude that CALEA applies to providers of "interconnected VoIP services." As defined in our recent VoIP E911 Order,107 interconnected VoIP services include those VoIP services that: (1) enable real-time, two-way voice communications; (2) require a broadband connection from the user's location; (3) require IP-compatible customer premises equipment; and (4) permit users to receive calls from and terminate calls to the PSTN.108 We find that providers of interconnected VoIP services satisfy CALEA's definition of "telecommunications carrier" under the SRP and that CALEA's Information Services Exclusion does not apply to interconnected VoIP services. **To be clear, a service offering is "interconnected VoIP" if it offers the capability for users to receive calls from and terminate calls to the PSTN; the offering is covered by CALEA for all VoIP communications, even those that do not involve the PSTN. Furthermore, the offering is covered regardless of how the interconnected VoIP provider facilitates access to and from the PSTN, whether directly or by making**

About Me (Full Bio)

CTO, VP, Founder of TMC Labs; B.S. Computer Engineering, 11 years telecom experience, 25 years programming, tinkering with and breaking computers. Gadgets are a favorite topic on this blog

VoIP and Gadget Blog Home Page

Search this site:

Search

Recent Entries

- LignUp FastLign Alliance to speed up VoIP deployment
- Linksys CIT200 Skype phone review
- Interesting new VoIP product
- Yahoo podcast service
- The fracturing of the Internet
- AOL offers presence to bloggers
- Wow, AOL buying Weblogs, Inc
- Satellite VoIP service
- SIPThat joins TMC bloggers
- Global IP Sound goes after VoIP hardware

Categories

- Call Center and CRM(25)
- Google(31)
- Mobile Phones(3)
- Outside News(5)
- Personal and Humor(44)
- Technology and


Skype - The whole world can talk for free. - Mozilla Firefox
skype
The whole world can talk for free.
180,951,842 downloads
Home
Products
Download
Community
Store
Help
Company
With Skype you can talk to anyone, anywhere for free. Forever.
Watch our little introduction movie to find out more.
Download Skype
Skype is a little program for making free calls over the internet to anyone else who also has Skype. It's free and easy to download and use, and works with most computers. Download Skype now or learn more about Skype (incl. screenshots).
Other nice Skype ideas
Skype Stories
Tell us your story
With SkypeOut, you can use Skype to call ordinary phone numbers all over the world.
Learn more
SkypeIn is a real phone number your friends can call. You pick up the call in Skype.
Learn more
Skype is in the air
Skype wedding
Thank you very much for this software which is really helpful for

انتهى