إدارة شبكات الاتصال وأمنها

الوحدة السابعة

تشفير المفتاح العام والتوقيع الرقمي

Public-key Cryptography & Digital Signature

مبادئ تشفير المفتاح العام
Public-Key Encryption Concepts

- **يعتمد على مبدأ استخدام مفتاحين**
  - المفتاح العام Public Key للتشفير
  - المفتاح الخاص Private Key لفك التشفير
- **بين المفتاحين علاقة رياضية معقدة ليصعب الوصول لأحدهما من خلال الآخر**
- **شروط أمن وفعالية استخدام المفتاح العام**
  - أن تكون عملية التشفير سهلة حسابياً (اختصار الوقت)
  - أن تكون عملية فك التشفير لمن يملك المفتاح الخاص سهلة أيضا
  - أن تكون عملية فك التشفير لمن لا يملك المفتاح الخاص صعبة حسابياً تستلزم وقتاً طويلاً حتى بمعرفة المفتاح العام
- **يتم إصدار شهادة للمستخدم بمفتاحه العام لمواجهة خطر التنكر**

استخدامات تشفير المفتاح العام
Applications of Public-Key Encryption

- **التشفير**
  - يستخدم المرسل المفتاح العام K الخاص بالمستقبل لتشفير الرسالة
  - يستخدم المستقبل مفتاحه الخاص K’ لفك التشفير
  - تستغرق خوارزمية تشفير المفتاح العام وقتا أطول نسبيا مقارنة بالخوارزميات التماثلية
- **تبادل المفاتيح السرية**
  - يتم تشفر المفاتيح التماثلية بالمفتاح العام وترسل مع الرسالة المشفرة–تماثلياً أو قبلها
- **التوقيع الرقمي**
  - يمنع خطر التنكر والإنكار

استخدامات تشفير المفتاح العام
Applications of Public-Key Encryption

- **التوقيع الرقمي ...**
  - يتم تشفير ملخص للرسالة بدالة الهاش Hash Function ويتم إرسال قيمته مع الرسالة إلى المستقبل
    - إذا حسب المستقبل قيمة مغايرة للقيمة المرسلة ذلك يعني تغير محتوى الرسالة
  - يشفرها المرسل بمفتاحه الخاص K' ، ويفك تشفيرها المستقبل بمفتاح المرسل العام K
    - بهذا يطمئن المستقبل لعدم تنكر المرسل وأن الرسالة وصلت سليمة
  - عند تسلم المستقبل للرسالة وقيمة الهاش يقوم بـ
    - فك تشفير قيمة الهاش بمفتاح المرسل العام
    - حساب قيمة الهاش بنفس الدالة المتفق عليها
    - ومقارنتها بالقيمة المرسلة

استخدامات تشفير المفتاح العام
Applications of Public-Key Encryption

- توقيع الرسالة وتشفيرها معاً – استخدام مرحلتي تشفير :

1. **تشفير الرسالة بمفتاح المستقبل العام للمحافظة على سرية محتواها**
2. **تشفير قيمة الهاش للرسالة بمفتاح المرسل الخاص كتوقيع رقمي**

– لحل بطء مرحلتي التشفير، يتم تشفير قيمة الهاش بالمفتاح الخاص، أما الرسالة فتشفر بإحدى خوارزميات التشفير التماثلي

التشفير باستخدام العمليات الحسابية – الجمع

- محاكاة شيفرة قيصر: ولكن يتم استخدام مفتاحين واحد للتشفير K وآخر لفك التشفير K’ بحيث

$$C = (P + K) \bmod 26 \quad , \quad P = (C + K') \bmod 26$$

$$P = (((P + K) \bmod 26 \; + \; K') \bmod 26$$

– K أقل من 26: $K = K \bmod 26$

– تعتمد قيمة K’ على قيمة K بحيث

$$(K + K') \bmod 26 = 0$$

مثال التأكد ص 225

التشفير باستخدام العمليات الحسابية – الضرب

- تشبه التشفير بعملية الجمع ولكن وفقاً للمعادلات:
  - $C = (P*K) \bmod 26$
  - $P = (C*K') \bmod 26$
- تعتمد قيمة K’ على قيمة K بحيث

$$K*K' \bmod 26 = 1$$

- الجدول ص 257
  - جميع قيم K و K’ وناتج العلاقة بينهما في المدى 0–25
- مثال ص 256
- قيم المفاتيح من 0–25 تجعلها عرضة لهجوم القوة الجبارة

التشفير باستخدام العمليات الحسابية – الضرب

- ليست كل القيم 0–25 صالحة لـ K
  - يجب أن تكون العلاقة K*P mod 26 قابلة للعكس Reversible
    - الجدول ص 259
    - يجب أن تكون قيمة K أولية نسبية لـ 26 (ليس بينهما عوامل أولية مشتركة)
- الدالة Φ(n) تمثل عدد الأعداد الأولية النسبية للعدد n
  - Φ(26) = 12 : 1و3و5و7و9و11و15و17و19و21و23و25
  - لتجنب اختيار قيمة غير مناسبة لـ K نختار عدد أولي لمقام باقي القسمة. فتعطينا عدد احتمالات أكثر لـ K (0 : n-1)
    - إذا كان n عدد أولي فإن Φ(n) = n-1

تشفير أكثر من حرف معاً ككتلة واحدة

- تعاني عملية الضرب في التشفير من مشكلتين : أحادية الأبجدية (تكرار الأنماط) وتتعرض لهجوم القوة الجبارة
- لزيادة عدد المفاتيح الممكنة
  - تشفير كتلة من حرفين أو أكثر وتعطى الكتلة كاملة رمزاً رقمياً واحداً.
  - يزيد عدد المفاتيح الممكنة K و K’ كلما ازداد حجم الكتلة الواحدة
- لتشفير الكتلة : $C = P * K \bmod n$
  - حيث n عدد الكتل الممكن تشكيلها
  - يتم تحديد عدد أولي قريب من N كمقام لعملية باقي القسمة
  - مثال جدول ص 261

خوارزمية RSA

- تستخدم العملية الحسابية الأسية Exponential
- تتم عملية التشفير وفك التشفير كالتالي

$$C = P^K \bmod n$$

$$P = C^{K'} \bmod n$$

- للتحقق من صحة التشفير وفك التشفير على النحو التالي

$$P = (P^K \bmod n)^{K'} \bmod n$$

أي أن

$$P = P^{K*K'} \bmod n$$

وعليه يجب أن

$$P < n \quad \& \quad K * K' \bmod \Phi(n) = 1$$

& K is Relatively Prime for $\Phi(n)$

خوارزمية RSA

- يستخدم للتشفير المفتاح العام للخوارزمية وهو K و n معاً
- يتم فك التشفير باستخدام الفتاح الخاص K’ بالإضافة إلى K من المفتاح العام (للمرسل)
- الخصم يعلم قيمة المفتاح العام أي K و n كما يعلم أن
  $K * K' \bmod \Phi(n) = 1$
- يجب أن لا يستطيع الخصم حساب $\Phi(n)$ لاستنتاج K’
  - حساب $\Phi(n)$ يحتاج إلى تحليل عوامل جميع الأعداد أقل من n
  - يجب تكبير قيمة n ما أمكن

خوارزمية RSA

- حساب $\Phi(n)$ والتحقق من $K * K' \bmod \Phi(n) = 1$
  - نفترض a و b عددان أوليان حيث أن
    - $n = a * b$
  - وحسب القانون $\Phi(n) = \Phi(a) * \Phi(b)$ فإن
    - $\Phi(n) = (a-1) * (b-1)$
  - الخطوة الأولى في تحديد المفتاحين العام والخاص
    - إختيار قيم العددين a و b كبير جداً وأن على المتراسلين الحفاظ على سريتهما كي لا يسهل حساب $\Phi(n)$
- كلما زادت قيمة n تصعب عملية التحليل إلى عوامل Factorization Problem

خطوات تشكيل المفتاحين العام والخاص

1. اختر رقمين أوليين a و b
2. احسب قيمة n حيث : $n = a * b$
3. احسب $\Phi(n)$ حيث : $\Phi(n) = (a-1) * (b-1)$
4. اختر قيمة أولية لـ K بحيث يكون أقل من $\Phi(n)$
5. اختر قيمة لـ K’ بحيث : $K * K' \bmod \Phi(n) = 1$

مثال

- الكتاب

جوانب عملية

- خوارزمية RSA تتطلب القيام بالعديد من عمليات رفع القوى x^n يتسبب تطبيقها في مشكلتين
  - تنفيذ التعبير الرياضي x^n يأخذ وقتاً طويلا
    - يمكن اختصار عمليات الضرب. كمثال حساب X^{17} كالتالي

$$X^2 = X * X \text{ ,,, } X^4 = X^2 * X^2 \text{ ,,, } X^8 = X^4 * X^4 \text{ ,,, } X^{16} = X^8 * X^8$$

$$X^{17} = X^{16} * X$$

  - تمثيل الأرقام الكبيرة في الذاكرة حيث أن القيمة P^K ذات حجم هائل
    - يمكن استغلال اختصارات باقي القسمة لحل المشكلة

$$(a * b) \bmod n = (a \bmod n) * (b \bmod n) \bmod n$$

حيث أننا بحاجة إلى حساب $P^K \bmod n$ بدلاً من حساب P^K فتبقى جميع القيم أصغر من n

اعتداءات تتعرض لخوارزمية RSA

- كمعظم الخوارزميات فهي عرضة لهجوم القوة الجبارة Brute Force Attacks
  - يمكن زيادة حجم المفتاح .... لحل المشكلة
- الاعتداءات الرياضية Mathematical Attacks
  - التركيز على استنتاج القيم (العوامل) الأولية Factorization Problem a,b
  - كلما زاد حجم n ازداد الوقت اللازم لحسابها
  - ينصح أيضا بتغيير المفتاح من فترة إلى أخرى
- الاعتداءات التوقيتية
  - تعتمد على تقدير الوقت اللازم لفك التشفير وعلاقته بطول المفتاح
  - لتجنب هذا الخطر يمكن إضافة وقت عشوائي Delay قبل النتيجة

التوقيع الرقمي والتحقق من المصداقية

- **يتم تشفير الرسالة بالمفتاح الخاص ويفك تشفيرها المستقبل بالمفتاح العام للمرسل**
- **إذا حصل المستقبل على نص سليم المعنى يستنتج**
  - المرسل هو صاحب المفتاح بالفعل
  - الرسالة لم تعدل من قبل طرف ثالث
  - لا يستطيع المرسل إنكار رسالته التي وقعها بمفتاحه الخاص
- **بما أن خوارزمية المفتاح العام ليست سريعة في التشفير وفك التشفير**
  - يتم حساب قيمة تسمى هاش Hash Value مستخلصة من الرسالة ثم تشفر القيمة وترسل مع الرسالة فتمثل البصمة الرقمية Finger Print
  - يتم حساب قيمة دالة الهاش n كما يلي $n = H(m)$
- **يمكن تشفير الرسالة الأصلية بالمفتاح العام أو بالتشفير التماثلي وترسل مع الهاش المشفرة بالمفتاح الخاص**

مواصفات دوال الهاش الجيدة

- أن تنتج الدالة عدداً ثابتا من الخانات Bits بغض النظر عن حجم الرسالة
- إذا علمت n يصعب حساب x حيث n = H(x) أو يصعب حساب n إذا علمت H(x)
  - كي لا يحدد الخصم القيمة (البصمة) ويستبدلها برسالة مساوية
- صعوبة عمل رسالة أخرى لها نفس البصمة
  - لتجنب اعتداء يدعى عيد الميلاد Birthday Attak
- من أهم دوال الهاش المستخدمة -MD5 , SHA-1 , RIPEMD

إدارة شبكات الاتصال وأمنها

الوحدة الثامنة

أمن البيانات في الحياة العملية

Data Security in Practice

إدارة المفاتيح

- يوزع المفتاح السري في التشفير التماثلي
- يوزع المفتاح العام في التشفير غير التماثلي
  - لا توزيع للمفتاح الخاص
- توزيع المفاتيح العامة

شهادات المفاتيح العامة Public Key Certificate

- شهادة تضمن ملكية المفتاح العام لصاحبه الأصلي
- يتم تصديق الشهادة بالمفتاح الخاص لجهة إصدار الشهادة
  - يتحقق المستقبل من مصداقيتها بفك التشفير باستخدام المفتاح العام لجهة الإصدار
- تحتوي الشهادة على معلومات منها:
  - رقم الإصدار
  - اسم صاحب المفتاح
  - تاريخ إصدار الشهادة
  - المفتاح العام
  - نوع خوارزمية التشفير المكن استخدامها
  - تاريخ الانتهاء

شهادات المفتاح العام

- نوعان من شهادات المفتاح العام

1. شهادات شخصية Personal Certificate
   - إثبات للأفراد بأنهم أصحاب المفاتيح بالفعل
     - يتم التعامل بها مع المواقع الخاصة بمجموعة معينة أو المواقع التي تتطلب التحقق من هوية المستخدم
2. شهادات مواقع الويب Web Site Certificate
   - إثبات سرية ومصداقية الموقع عند إرسال المعلومات الخاصة لمستخدميه، وسلامة الموقع من أجل عمليات التحميل السليمة

- جهات اصدار المفاتيح العامة
  - بعضها باجر وبعضها مجانية مثل Thawte و Verisign and Comodo
  - تحتوي مستكشفات الإنترنت على المفاتيح العامة لهذه الجهات للتحقق من الشهادات المصدرة

خطوات الحصول على شهادة المفتاح العام

- ص 290

توزيع المفاتيح السرية

- طريقتين لتوزيع المفاتيح السرية
  - توزيع المفاتيح بواسطة مركز خاص (طرف ثالث)
  - تبادل المفاتيح بين المستخدمين (بدون طرف ثالث)

توزيع المفاتيح السرية بواسطة مركز خاص

- تتطلب وجود طرف ثالث موثوق به من قبل طرفي الاتصال Key Distribution Center KDC
- يمنح كل مستخدم مفتاحاً رئيسياً لغرض تبادل الرسائل مع المركز
- يطلب المرسل من المركز مفاتيح مؤقتة لجلسة تشفير واحدة
- يرسل المركز المفاتيح المؤقتة مشفرة ليقوم المرسل بفك تشفيرها بمفتاحه الرئيسي.

توزيع المفاتيح السرية بواسطة مركز خاص

- خطوات الحصول على مفتاح سري مؤقت

1. طلب المرسل A المفتاح المؤقت Ks من المركز. يحتوي الطلب على:
   - عنوان الطلب request
   - الرقم التسلسلي للطلب N1
2. يقوم المركز بإرسال المفتاح المؤقت برسالة مشفرة باستخدام المفتاح الرئيسي للمرسل:

$$E_{Ka}\ (Ks \mid\mid N1 \mid\mid request \mid\mid E_{Kb}\ (Ks \mid\mid IDA))$$

   - N1 تساعده في تحديد الطلب (اذا أرسل عدة طلبات)
   - Request ليتحقق بأن الطلب نفسه لم يتغير
   - رسالة مشفرة إلى المستقبل B تتضمن نسخة من المفتاح المؤقت ومعلومات معرفة بالمرسل

توزيع المفاتيح السرية بواسطة مركز خاص

- **خطوات الحصول على مفتاح سري مؤقت...**

3. يقوم المرسل بفك التشفير واستخراج رسالة المستقبل (E_{KB} (Ks || ID_A) وإرسالها
4. يقوم المستقبل بفك تشفير الرسالة والحصول على المفتاح المؤقت Ks

– **وللتأكد من صحة الرسالة وحداثتها يتم القيام بثلاث خطوات إضافية**

5. يقوم المستقبل بتشفير قيمة عددية N2 باستخدام Ks وإرسالها إلى المرسل
6. يقوم المرسل بإجراء عملية حسابية (دالة) متفق عليها على القيمية العددية N2 ويرسل النتيجة إلى المستقبل
7. يقوم المستقبل بمقارنة ناتج الدالة مع القيمة المرسلة

تبادل المفاتيح السرية بدون طرف ثالث

- يتبادل أطراف الإرسال المفاتيح السرية بطريقتين:
  - توزيع المفاتيح المؤقتة باستخدام مفاتيح رئيسية سرية
  - توزيع المفاتيح السرية باستخدام طرق تشفير المفتاح العام

توزيع المفاتيح المؤقتة باستخدام مفاتيح رئيسية سرية

- يشترك كل زوج من المستخدمين بمفتاح سري رئيسي K_{MK} يستخدم في تبادل المفاتيح المؤقتة. وتلخص الخطوات التالية

1. يرسل A طلباً إلى B لمفتاح مؤقت ويرسل معه N1
2. يشكل B المفتاح المؤقت Ks ويرسله مشفراً باستخدام K_{MK} وتحتوي الريالة رد request وقيمة F(N1) وقيمة جديدة N2
3. يقوم A بفك التشفير وإرسال F(N2) مشفرة بـ Ks

– بإرسال N1 وN2 والدوال يطمئن الطرفان أن الرسالة ليست قديمة أعاد إرسالها الخصم

- مشكلة هذه الطريقة أنها تتطلب عدداً كبيراً من المفاتيح n(n-1)/2

– حيث n عدد لمستخدمين

توزيع المفاتيح باستخدام طرق تشفير المفتاح العام

- لا تتصلب قيام الطرفين باختيار مفتاح سري رئيسي بينهما
- يتم اختيار مفتاح سري لتشفير الرسالة تماثلياً ثم تشفير الرسالة والمفتاح السري بالمفتاح العام للمستقبل
- يمكن أن يشفر المرسل المفتاح السري باستخدام مفتاحة الخاص (كتوقيع رقمي) ثم بالمفتاح العام للمستقبل

المواقع المناسبة للتشفير وفك التشفير في شبكات الحاسوب

- قنوات الاتصال عند استخدام شبكات الحاسوب أثناء التشفير وفك التشفير ذو صلة باعتداءات تحليل الأنماط فهي المكان المناسب لهجوم الخصم
- تصعب السيطرة على قنوات الاتصال لسببين
  - غالباً ما تكون خطوط الاتصال خارج السيطرة المادية لمستخدمي الشبكة
  - وجوب نقل البيانات في حالة مناسبة لتمريرها من خلال الموجهات
- قنوات الاتصال وأمنها
  - أسلاك معدنية Coaxial Cables و Twisted Pairs وهي الأكثر عرضة للاعتداءات
  - الموجات القصيرة Microwaves
  - كوابل الألياف الضوئية Fiber Obtic وه الأكثر أماناً

أنواع المواقع المناسبة للتشفير وفك التشفير

1. تشفير النهايات End-to-End Encryption
   - تقع مسئولية التشفير وفكه على عاتق المرسل والمستقبل
   - فوائد تشفير النهايات
     1. ان المستقبل فقط من يستطيع فك التشفير
     2. تعطي المستخدم حرية في استخدام خوارزمية التشفير
     3. تمكن المستقبل من التأكد من هوية المرسل
   - مشكلة هذه الآلية
     - لا يمكن للمرسل تشفير ترويسة الحزمة Packet لاحتوائها على عنوان المستقبل. فيستطيع الخصم تحديد المستقبل وتحليل أنماط الاتصال

أنواع المواقع المناسبة للتشفير وفك التشفير

2. تشفير طرفي قناة الاتصال
   - يشترك كل زوج من الموجهات بمفتاح سري
   - تكمن أهمية طريقة تشفير قناة الاتصال في أنها تسمح بتشفير الحزمة كاملة
   - مشاكلها
     - كل عقدة توجيه تستطيع فك تشفير الرسالة لمعرفة عنوان المستقبل
     - لا تعطي المستخدم حرية في اختيار خوارزمية التشفير
     - لا تمكن المستقبل من التحقق من هوية المرسل

يمكن التشفير بالطريقتين : تشفير النهايات ثم خط الاتصال

تحليل حركة المرور وأنماط الاتصال

- تحليل أنماط الاتصال يعطي الخصم القدرة على استنتاج محتوى الرسائل حيث:
  - الاتصال المتكرر يعني أن الطرفين يخططان لأمر ما
  - الرسائل القصيرة المتبادلة بسرعة تعني وجود تفاوض
  - الرسائل القصيرة تحمل الموافقة والعكس صحيح
  - تزداد الخطورة في الشبكات WAN حيث أن قنات الاتصال خارج السيطرة المادية

الإجراءات الوقائية

- من الصعب اكتشاف الاعتداء أو التنصت على شبكة الاتصال. ولكن من السهل إحباطها
- الإجراءات الوقائية في تشفير النهايات
  - توحيد حجم الرسائل
  - تتبادل الموجهات رسائل عشوائية طوال الوقت محددة أي الرسائل حقيقية وأيها عشوائية
- الإجراءات الوقائية في تشفير طرفي قنات الاتصال
  - اشغال الشبكة طوال الوقت بنفس المقدار

أمن الشبكة العنكبوتية Web Security

- يقصد بها الاتصال الآمن بين موقع الويب ومتصفح الإنترنت لدى المستخدم
- المستخدم بحاجة إلى التحقق من هوية الموقع إضافة إلى سرية طبقة الاتصال TLS Transport Layer Security"
- يهدف TLS إلى
  - عدم اطلاع الخصوم على المعلومات أو تعديلها
  - التأكد من هوية الموقع قبل إرسال المعلومات إليه

مراحل عمل سرية طبقة الاتصال TLS

1. **مرحلة التفاوض:**
   - تحديد الخوارزميات وطرق التحقق من الهويات للخادم والمخدوم
   - تبدأ عندما يقوم المستكشف بطلب عملية اتصال آمنة
   - يقدم المستكشف مجموعة من الخوارزميات ودوال الهاش التي يمكن أن يتعامل معها ثم يقوم موقع الويب بالاختيار وتبليغ المستكشف
2. **مرحلة التحقق من الهوية**
   - يقوم الموقع بإرسال شهادة المفتاح العام الخاصة به إلى المستكشف
   - بعض الحالات يطلب الموقع شهادة المفتاح العام من المستكشف
3. **مرحلة تبادل المفاتيح السرية**
   - يرسل المستكشف المفتاح السري إلى الموقع مشفر بالمفتاح العام للخادم
4. **مرحلة تبادل الرسائل المشفرة**
   - يقوم الطرفان بتبادل الرسائل المشفرة بالمفتاح السري

أمن البريد الإلكتروني

- الكتاب