Steganographyالإخفاء

- في عام ٢٠١١ قامت السلطات الألمانية باعتقال أحد أعضاء تنظيم القاعدة، وكانت بحوزته بطاقة ذاكرة محمية بكلمة مرور، وعليها فيلم وثائقي بالإضافة لبعض الملفات العادية الأخرى.
- بعد الفحص الجنائي للبطاقة والفيلم تبين وجود ما يزيد عن ١٤٠ ملفًا نصيًا داخل الفيديو، منها ملفات تضم خططًا مستقبلية للتنظيم. هذا ما يعرف بعلم إخفاء المعلومات أو Steganography
- Steganography كلمة إغريقية وتعني الكتابة الخفية covered writing وهي مكونة من مقطعين Stego وتعني الغطاء و graphia وتعني الكتابة.
- الهدف من الإخفاء هو تضمين رسالة سرية secret message داخل غطاء carrier

© 2017 - Wesam A. Hatamleh

Steganographyالإخفاء

- إذن :هو العلم الذي يهتم باخفاء المعلومات الرقمية داخل وسيط الكتروني دون احداث أي تشويه أو تعديل ملحوظ في هذا الوسيط"
- الرسالة المخفية قد تكون صريحة plain أو مشفرة encrypted digital data stream
- لنقل لدينا معلومات أو ملفات رقمية (نص، صورة، صوت) نريد ارسالها عبر الشبكة لكي تصل بشكل آمن إلى الطرف الآخر، ودعونا نطلق على تلك المعلومات والملفات بالرسالة السرية

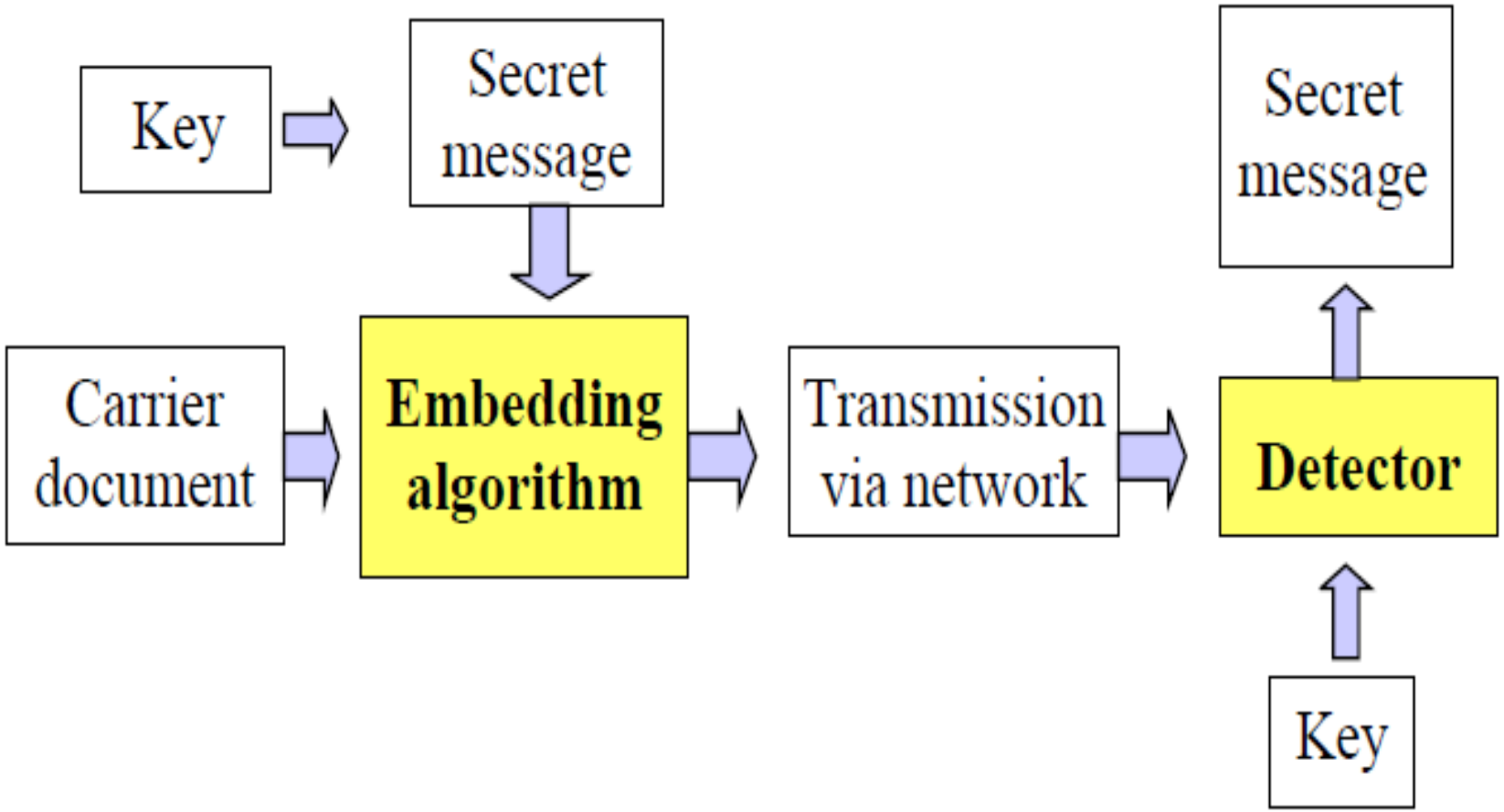
© 2017 - Wesam A. Hatamleh

Steganographyالإخفاء

- الرسالة السرية لن تُرسل بشكل مباشر ولكن يجب أن تدمج وتكون مخفية داخل رسالة الغطاء (أيضاً هذه الرسالة قد تكون نص، صورة، صوت) بشكل احترافي دون ترك أي أثر أو شك بأن هناك رسالة سرية داخل رسالة الغطاء.
- بالتالي تكون ناتج عملية الدمج هي رسالة التضمين والتي هي عبارة عن نسخة من رسالة الغطاء من حيث الشكل ولكنها تحتوي الرسالة السرية دون احداث أي شك أو ريب بوجودها.

© 2017 - Wesam A. Hatamleh

الإخفاءSteganography



© 2017 - Wesam A. Hatamleh

أساسيات التشفير الكتلي

- يعالج التشفير التدفقي(التسلسلي) **Stream Cipher** حرفاً أو ثنائية أو ثمانية من النص الصريح.
- يعالج التشفير الكتلي **Block Cipher** كتلة كاملة (مجموعة من الأحرف أو الثنائيات أو الثمانيات) من النص الصريح مرة واحدة.
- يفضل استخدام التشفير الكتلي نسبة لسرعته العالية نسبيا والمعرفة المناسبة بمطلوبات تصميمه.

© 2017 - Wesam A. Hatamleh

أساسيات التشفير الكتلي

- يتطلب تشفير الكتلة توفر البيانات قبل البدء في عملية التشفير.
- أساليب التشفير الكتلي المعتمدة على المفتاح المتناظر Symmetric-key block ciphers تعتبر من أكثر نظم التشفير أهمية واستخداما في كثير من التطبيقات اليوم.
- لا يوجد أسلوب تشفير كتلي واحد مناسب لجميع التطبيقات، حتى إنْ توفر مستوي عالٍ من الأمن والحماية لهذا الأسلوب.
- ومعرفة السبب في اختلاف مطلوب التشفير في التطبيقات المختلفة والتي قد تحددها والعوامل

© 2017 - Wesam A. Hatamleh

أساسيات التشفير الكتلي

- العوامل التي تحدد مطلوبات التشفير في التطبيقات المختلفة هي :
  - السرعة المطلوبة ومحدودية الذاكرة الذي قد ينتج من حجم برنامج التشفير وحجم البيانات والذاكرة السريعة cache memory.
  - آليات التنفيذ مثل العتاد والبرمجيات وكروت الرقائق chipcards.
  - اختلاف تسامح التطبيقات مع خواص صيغ التشغيل المختلفة.
  - ضرورة إيجاد التوازن بين الكفاءة والأمن.

© 2017 - Wesam A. Hatamleh

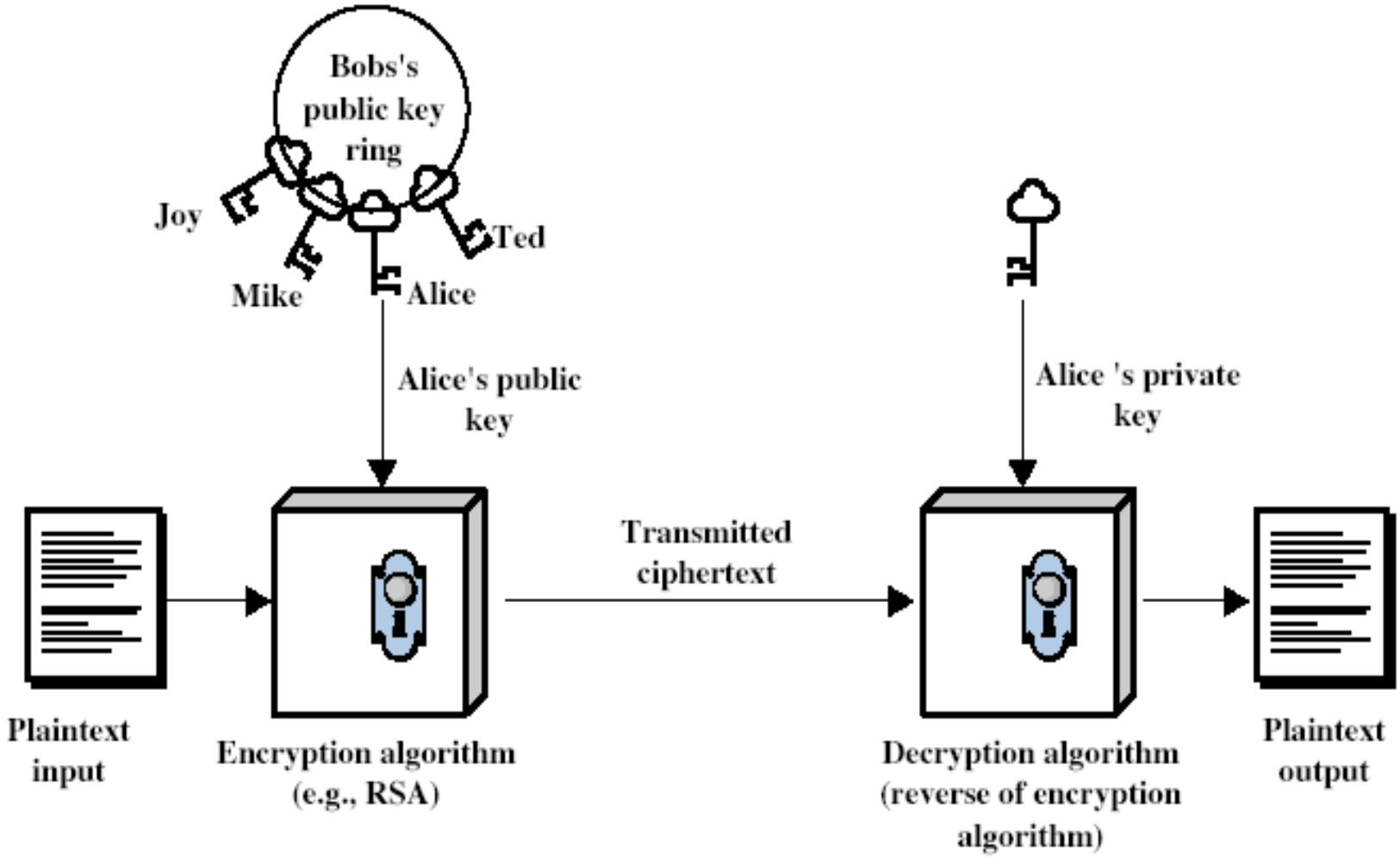
أساسيات التشفير الكتلي

تشفير فيزتل الكتلي Feistel block cipher

- تعتمد أغلب خوارزميات التشفير الكتلي المتناظر المستخدمة اليوم على أسلوب تشفير يعرف بتشفير فيزتل الكتلي **Feistel block cipher**.
- يعمل التشفير الكتلي على كتلة من النص الصريح حجمها n ثنائية لإنتاج كتلة في النص المشفر متساوية لها في الحجم.
- استخدام تشفير الإحلال يكون غير عملي بالنسبة للكتل الكبيرة، سواء من ناحية (التنفيذ) أو الأداء.
- يحتاج تشفير كتلة حجمها n ثنائية إلى مفتاح طوله $nx2^n$، فمثلاً لكتلة حجمها ٦٤ ثنائية، (وهذا الحجم يعتبر مثاليا للحماية من الهجمات الإحصائية)، تحتاج إلى مفتاح طوله $64x2^{64}$ ($2^{70} = 10^{21}$) ثنائية.
- لتفادي هذه المشكلة اقترح فيزتل تقريب لنظام التشفير الكتلي المثالي لمعالجة n ثنائية، يمكن بناءه من مكونات سهلة التحقيق.

© 2017 - Wesam A. Hatamleh

Public-Key Cryptography



© 2017 - Wesam A. Hatamleh

- ويكون المفتاح العام في التشفير اللامتماثِل معروفاً لدى أكثر من جهة أو شخص ، لتستطيع هذه الجهة تشفير أي رسالة ولكنها لا تُفتح إلا من صاحب الصلاحية بالمفتاح الخاص والذي هو سري. وفيما يلي أشهر الخوارزميات لهذا النوع من التشفير :

© 2017 - Wesam A. Hatamleh

خوارزمية ديفي و هيلمان (DH)

- خوارزمية ديفي وهيلمان تعتبر أول خوارزمية ذات مفتاح عام وكانت ١٩٧٦م وتعتمد على خاصية نظام اللوغاريتم الصحيح في تصميم نظام للتشفير. أن صعوبة كسر هذه الخوارزمية حسب ما هو معروف الآن تعادل صعوبة حل مسالة اللوغاريتم الصحيح إلا إنها خوارزمية بطيئة لأنها تعتمد على كثير من عمليات الرفع إلى قوة ، لذلك ينصح باستعمالها لتشفير الرسائل القصيرة وخصوصا المفاتيح التي تستخدمها خوارزميات أخرى ويتم تبادلها بين الإطراف المتراسلة.

© 2017 - Wesam A. Hatamleh