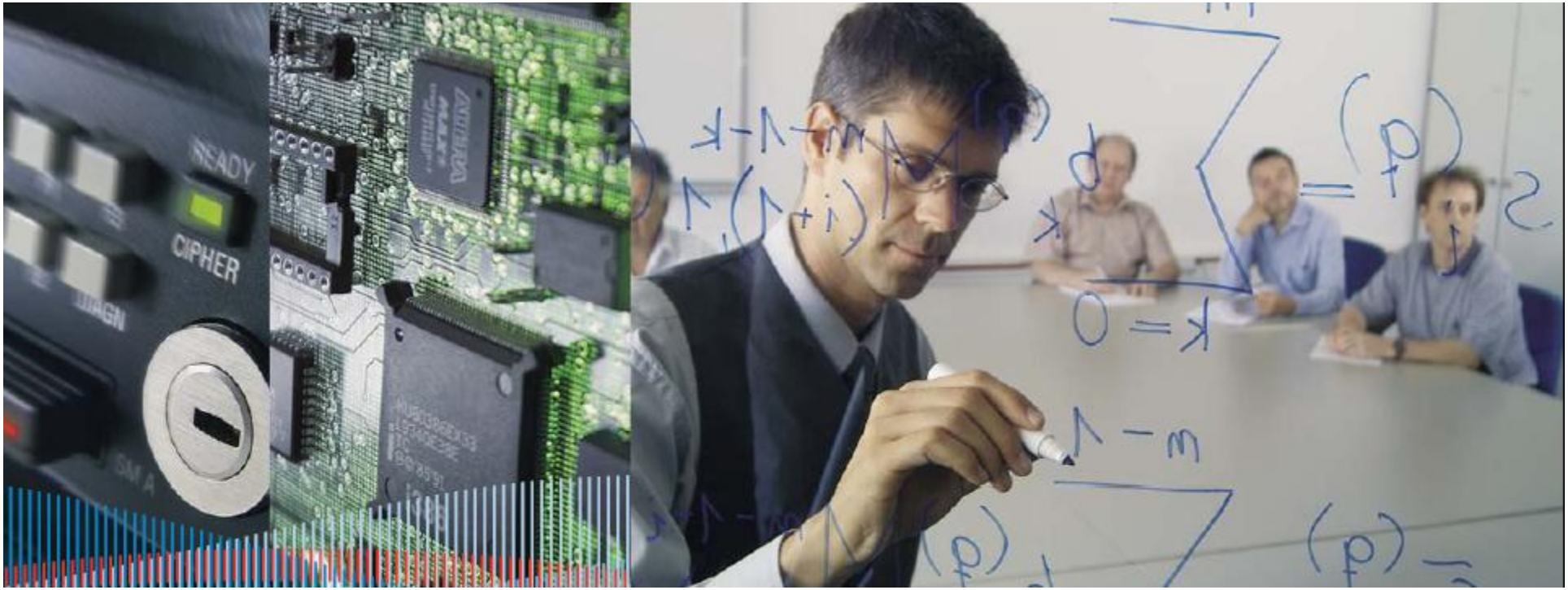


Information & Network Security
أمن المعلومات والشبكات

Eng. Fadi BAGHDADLIAN

Advanced Information Technology

bfadi@advitco.com

أصبح العالم يعتمد على الحواسيب والشبكات بكثرة

فقد أنتشر الوب والبريد الإلكتروني والتجارة الإلكترونية

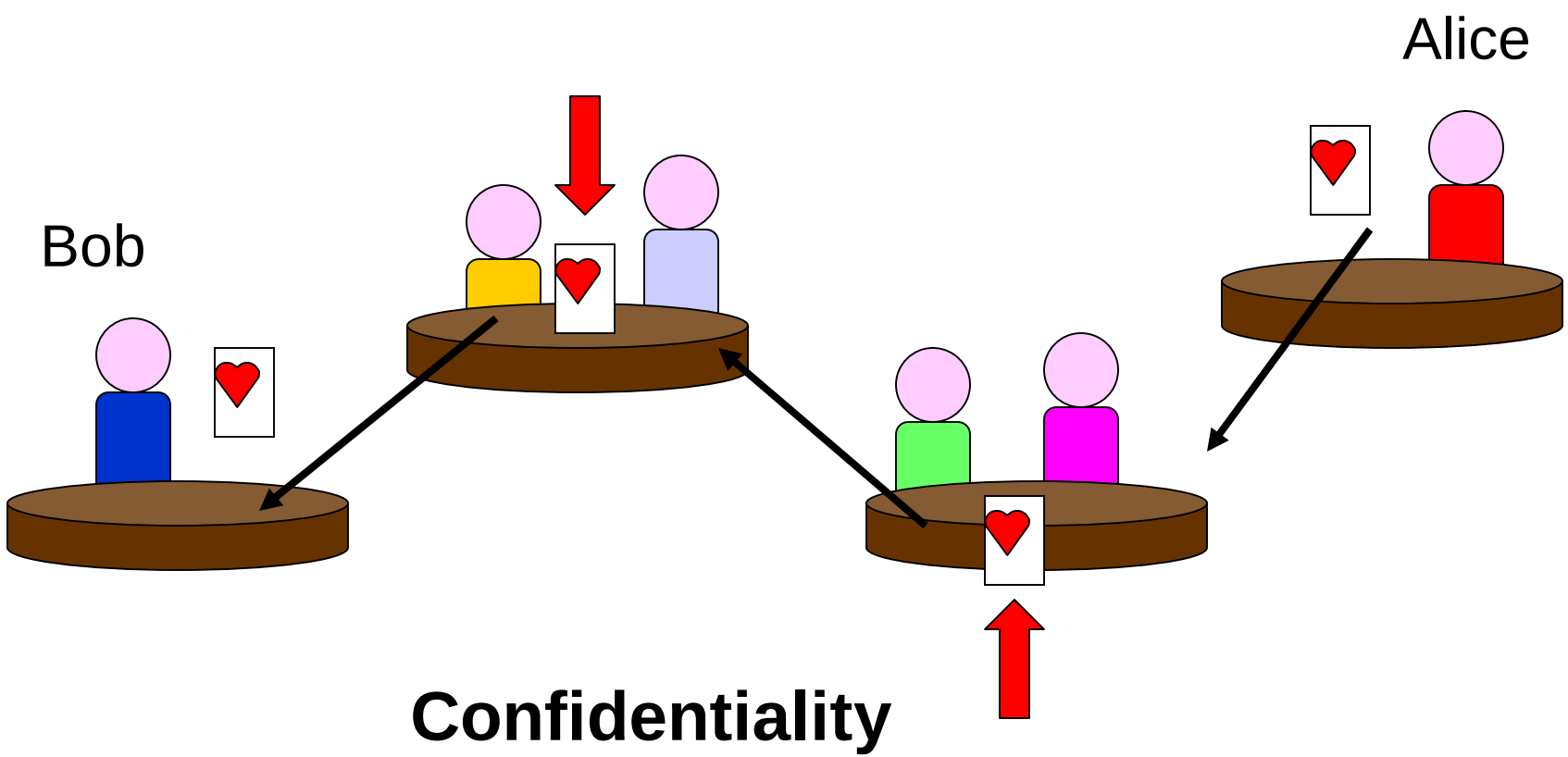
وأصبح الحاسب جزء لا يتجزأ من عالمنا.

ولكن هذا أدى لتشكيل خطر!

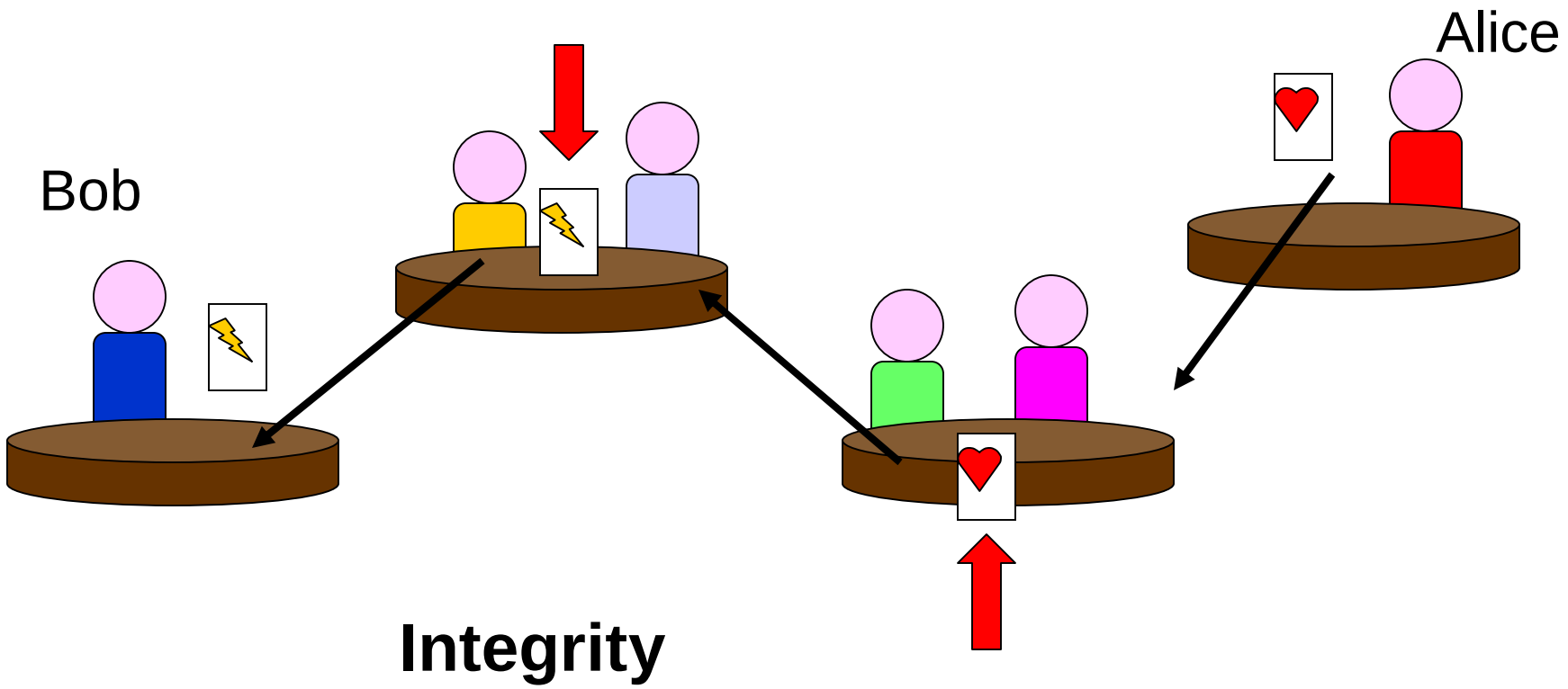
عناصر الأمان في أي نظام:

- Access control : منع الولوج
  - تحديد من يحق له الوصول للمعلومة
- Authentication : الاستيقان
  - التحقق من الهوية
- Privacy: السرية
  - حماية المعلومات الحساسة
- Integrity : سلامة المعلومات
  - ضمان سلامة المعلومات وعدم تعديلها
- Non-repudiation : عدم الإنكار
  - ضمان عدم الإنكار من المرسل

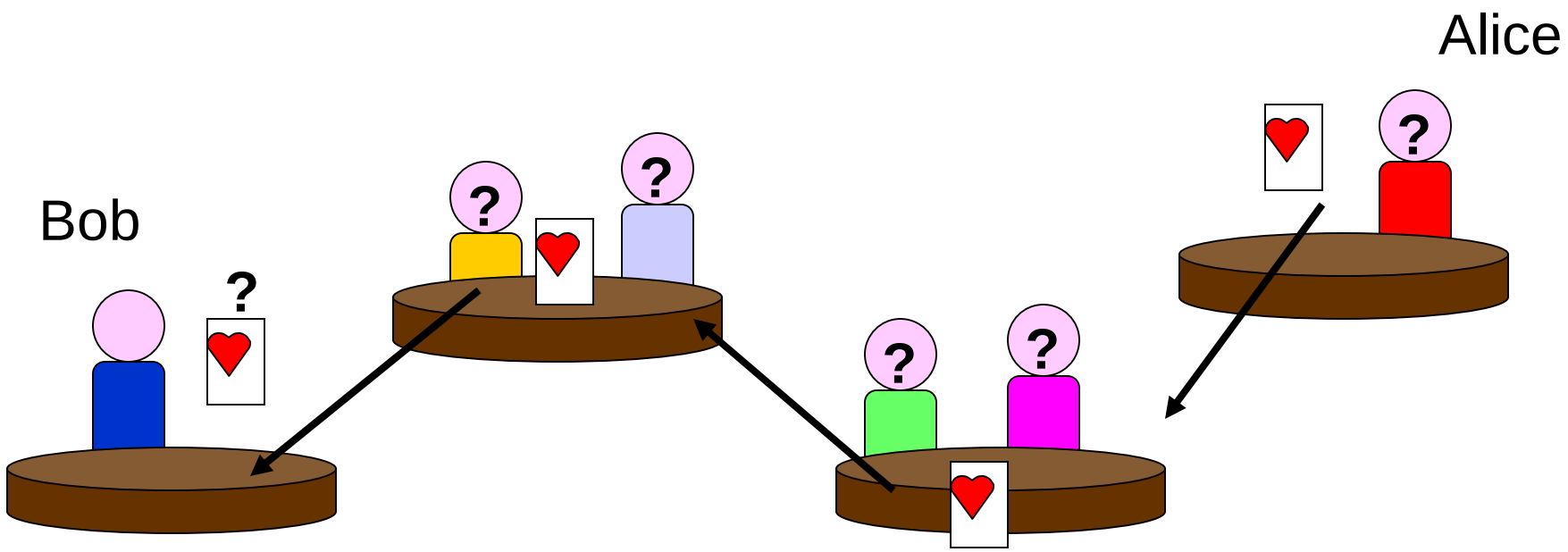
Case study : the restaurant



Case study : the restaurant (2)

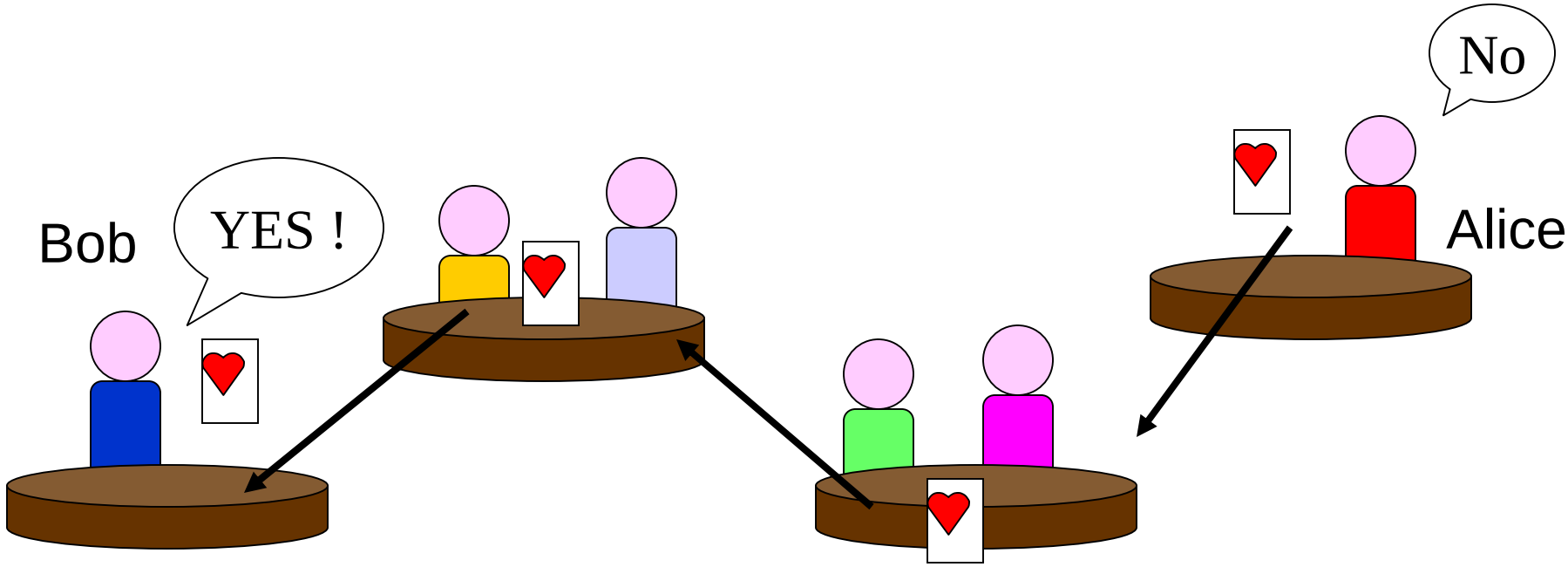


Case study : the restaurant (3)



Authentication

Case study : the restaurant (4)

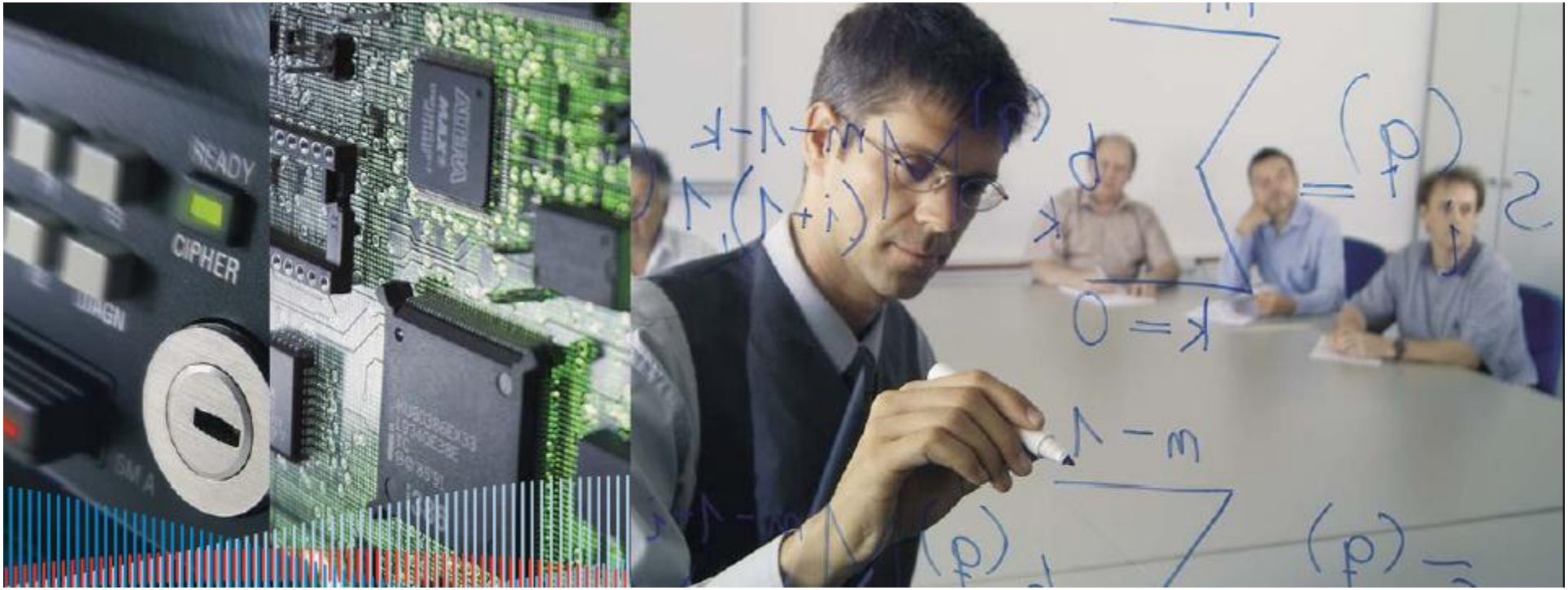


Non repudiation

Secure transactions means

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Provided by encryption



Cryptography

علم التعمية - التشفير

- Cryptography مأخوذة من اليونانية : kryptus + graphein : الكتابة المخفية
- استخدمت الكتابة المخفية منذ 1900 ق.م في مصر
- مصطلحات:

« plaintext النص الأصلي

« ciphertext النص المشفر

« Encryption التعمية أو التشفير

« Decryption فك التعمية

- Cryptanalysis : علم اختراق التعمية
- Cryptology : Cryptography + Cryptanalysis

خوارزميات التشفير لها المخطط التالي

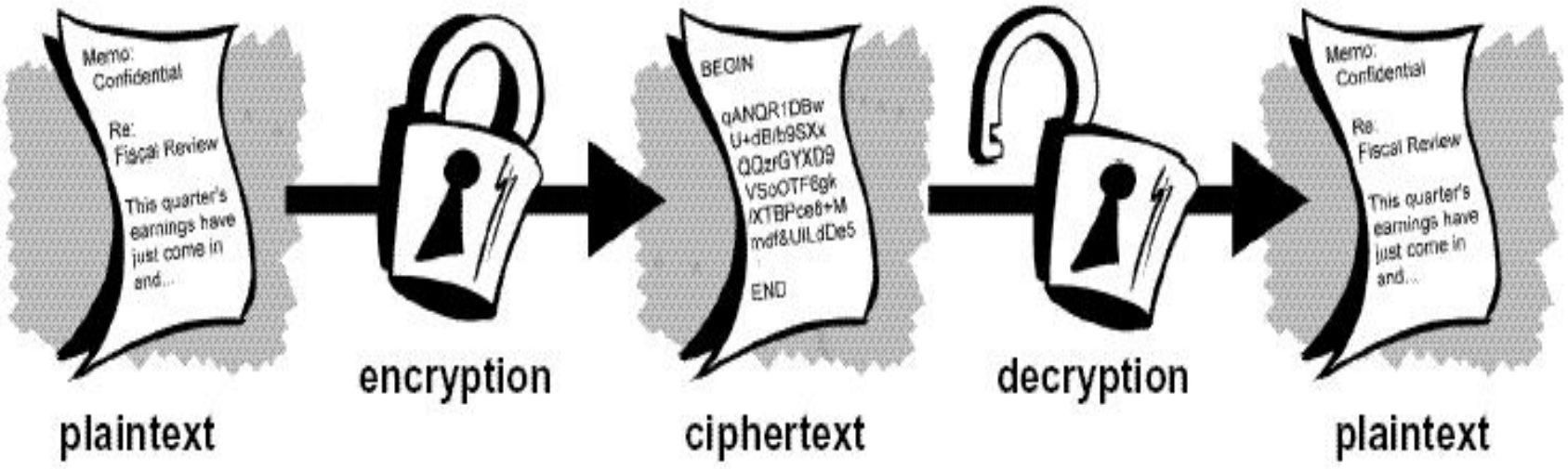


Figure 1-1. Encryption and decryption

طرق التشفير:

- خوارزمية التشفير غير معروفة $C=f(p)$
- خوارزمية التشفير معروفة ولكن مفتاحها غير معروف (وهي التي سنهتم بها $C=f_k(p)$)

أنواع خوارزميات التشفير:

- متناظرة (نفس المفتاح للتشفير ولفك التشفير)

DES-3DES-IDEA-blowfish-RC6-SKIPJACK-twofish-rijndael(AES)

- غير متناظرة (مفتاح للتشفير ومفتاح آخر لفك التشفير)

RSA-RABIN-MCELIECE-POHLIG HELLMAN-ElGAMAL

خوارزميات التشفير متناظرة المفتاح

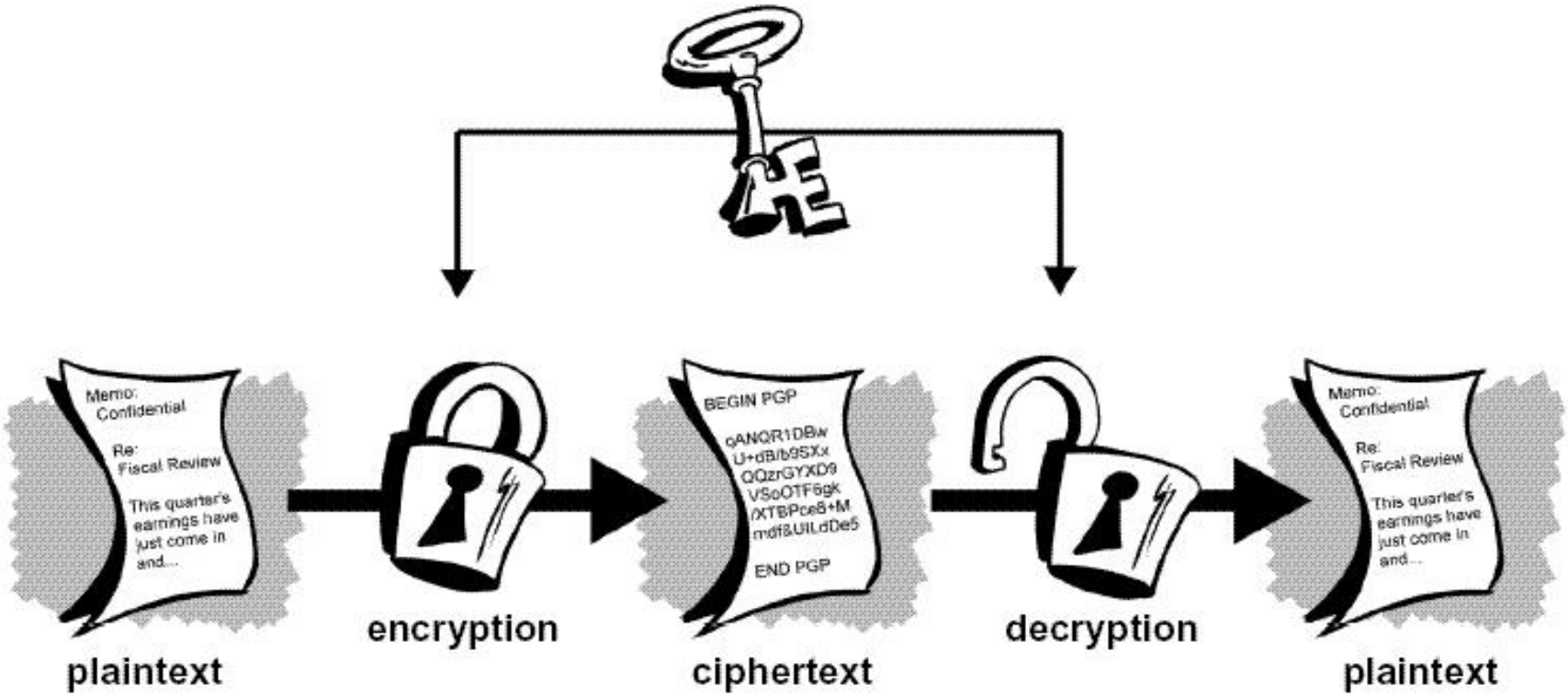


Figure 1-2. Conventional encryption

خوارزميات التشفير غير متناظرة المفاتيح

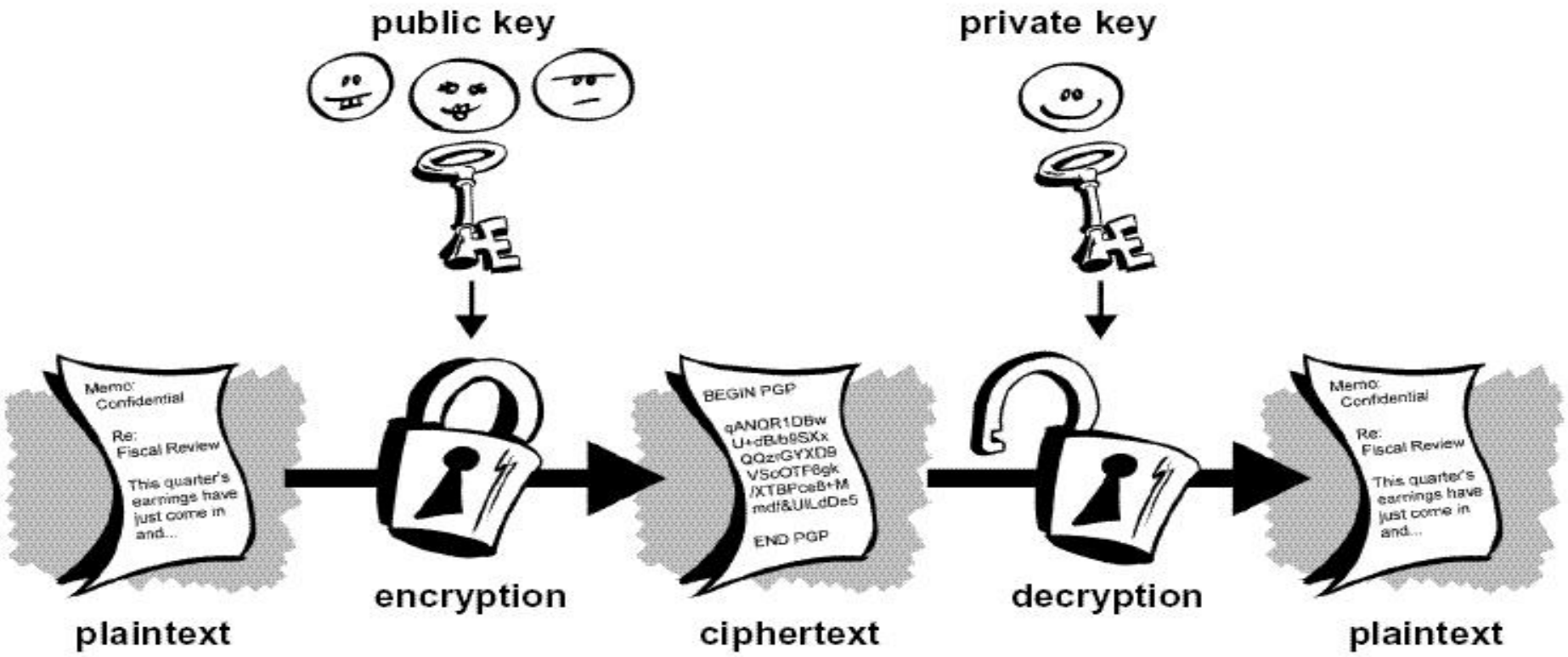


Figure 1-3. Public key encryption

التوقيع الإلكتروني

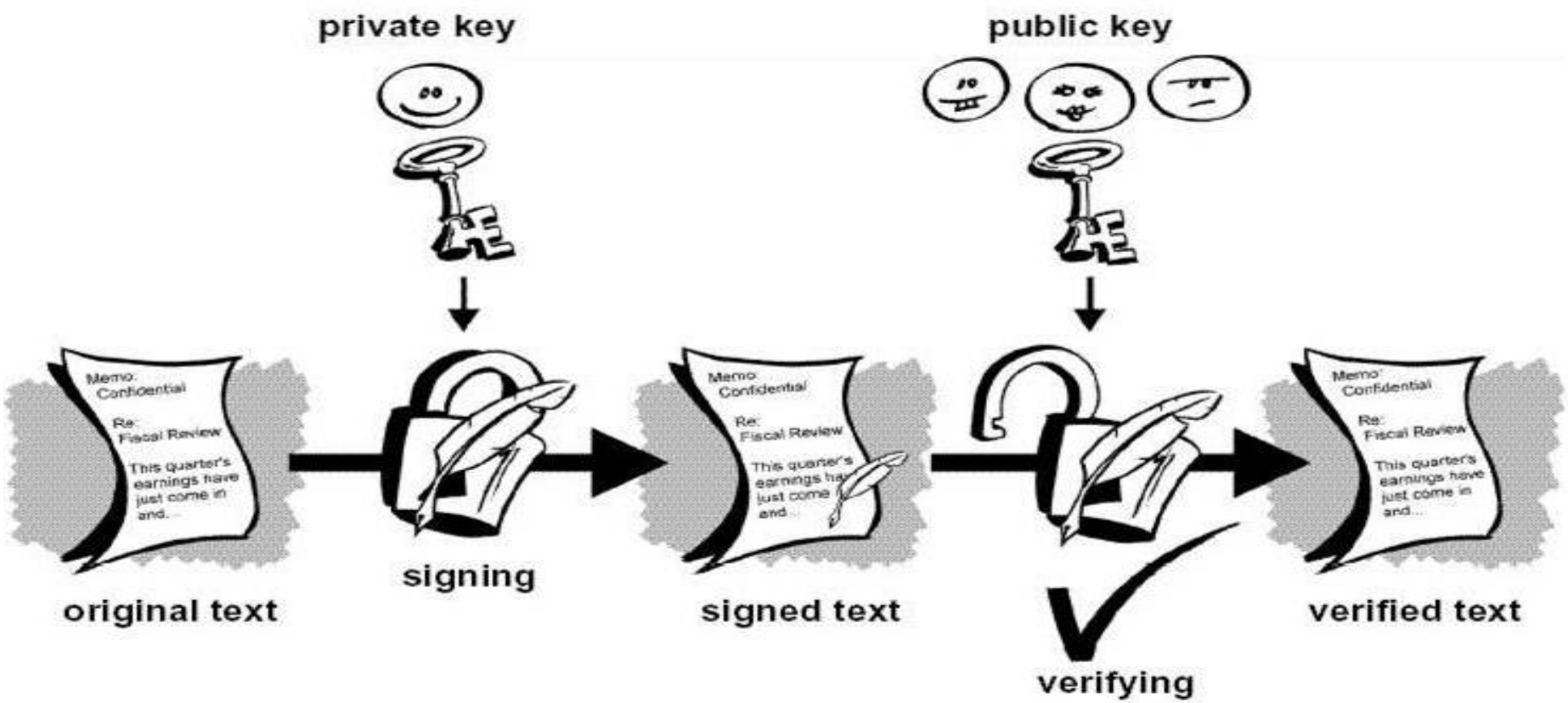


Figure 1-6. Simple digital signatures

مشاكل خوارزميات التشفير متناظرة المفاتيح

- تبادل المفتاح المشترك بين الأشخاص

مشاكل خوارزميات التشفير غير متناظرة المفاتيح

- بطئ الخوارزمية

مما أدى لظهور طرق لدمج الخوارزميات متناظرة المفاتيح مع اللا متناظرة المفاتيح : مثلPGP

التشفير باستخدامPGP

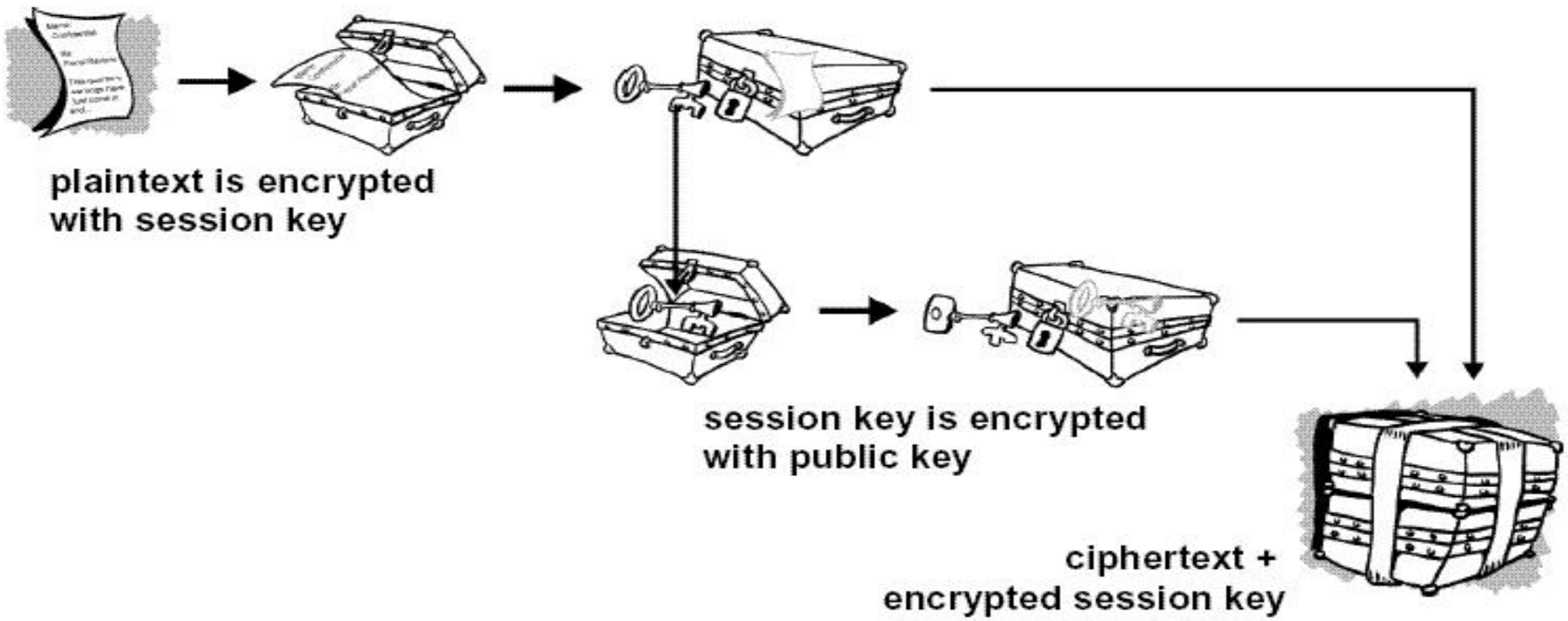


Figure 1-4. How PGP encryption works

فك التشفير باستخدامPGP

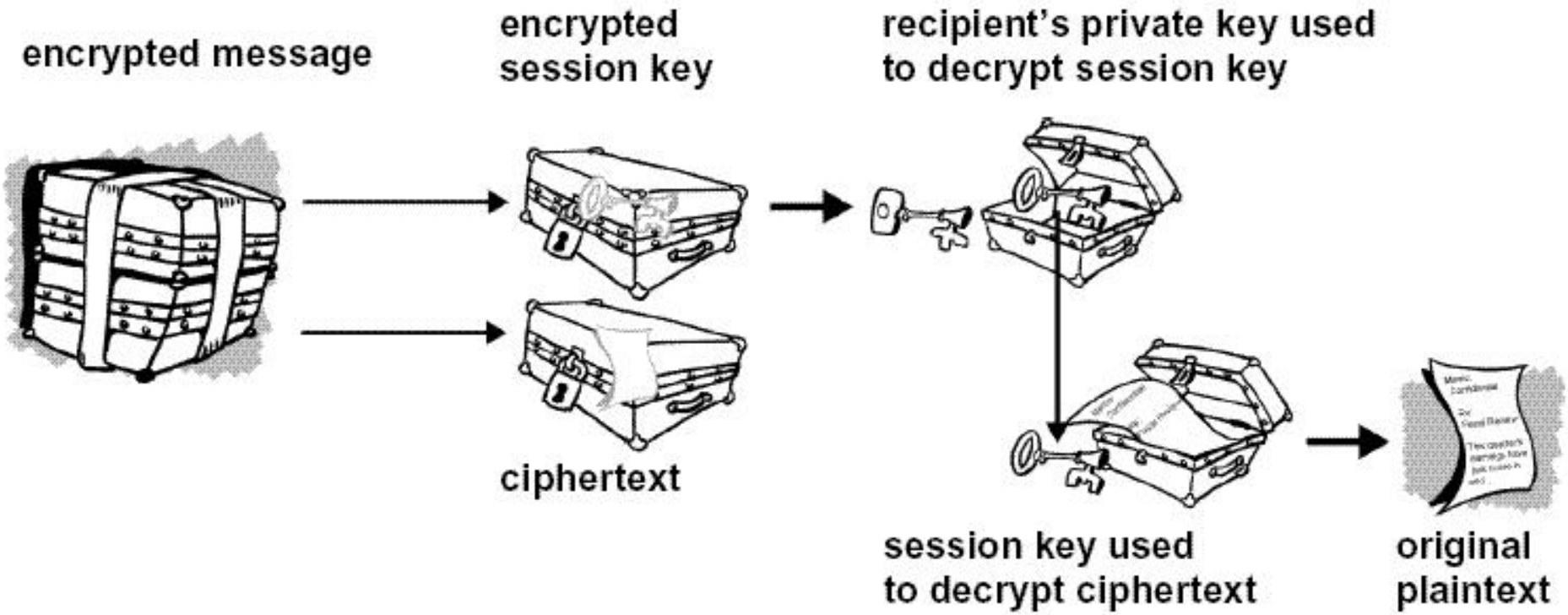
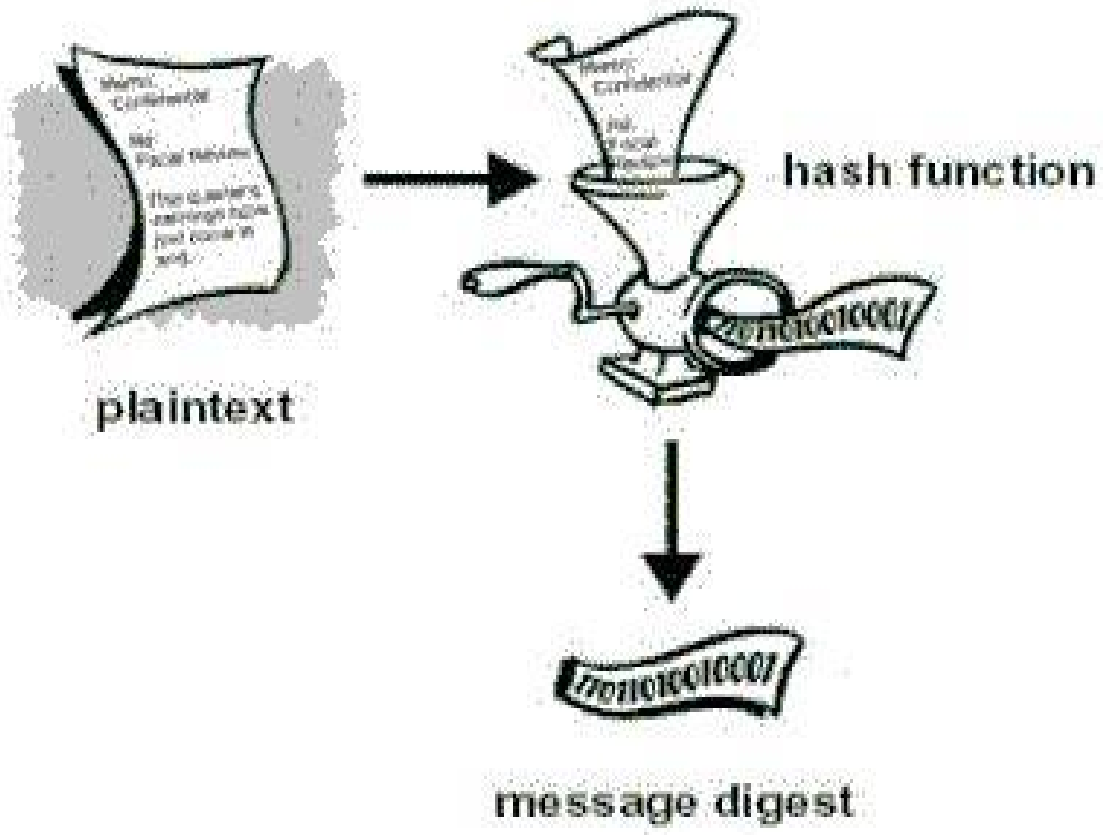


Figure 1-5. How PGP decryption works

خوارزمية Hash



- تحويل رسالة إلى 64 أو 128 بت
- تغيير بسيط بالرسالة يؤدي لتغيير كبير في نتيجة Hash
- من خوارزميات: Hash

N-Hash-MD4-MD5-SHA

التوقيع الإلكترونى باستخدام خوارزمياتHash

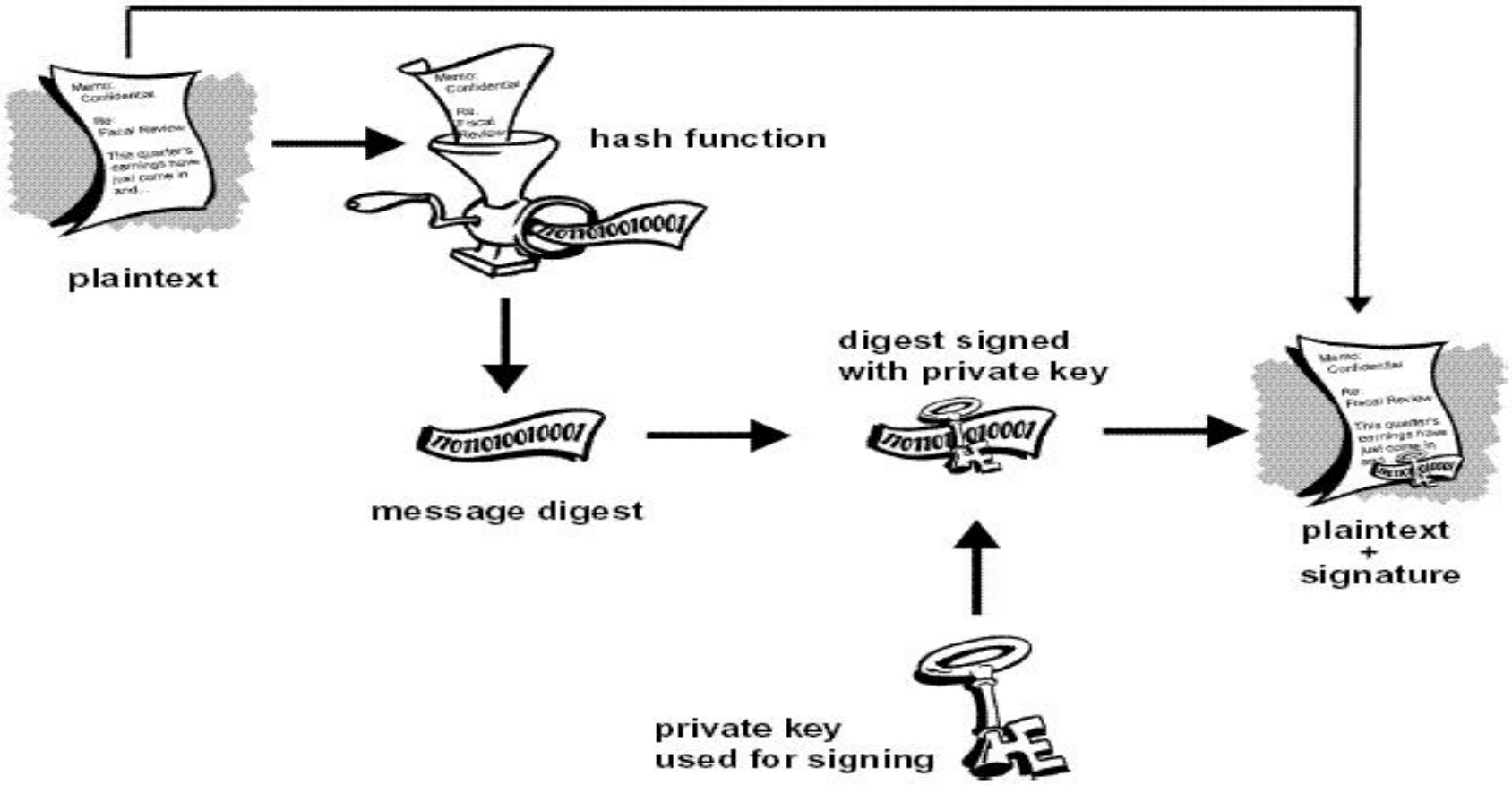


Figure 1-7. Secure digital signatures

مرجع الشهادات

Certificate Authority

- هي عبارة عن جهة موثوقة.
- تسجل المفاتيح العامة للمشتركين بقالب يسمى الشهادات .Certificate
- تسجل اسم المشترك و رقم هويته وتاريخ المنح والصلاحية.
- توقع الشهادات بمفتاحها الخاص.

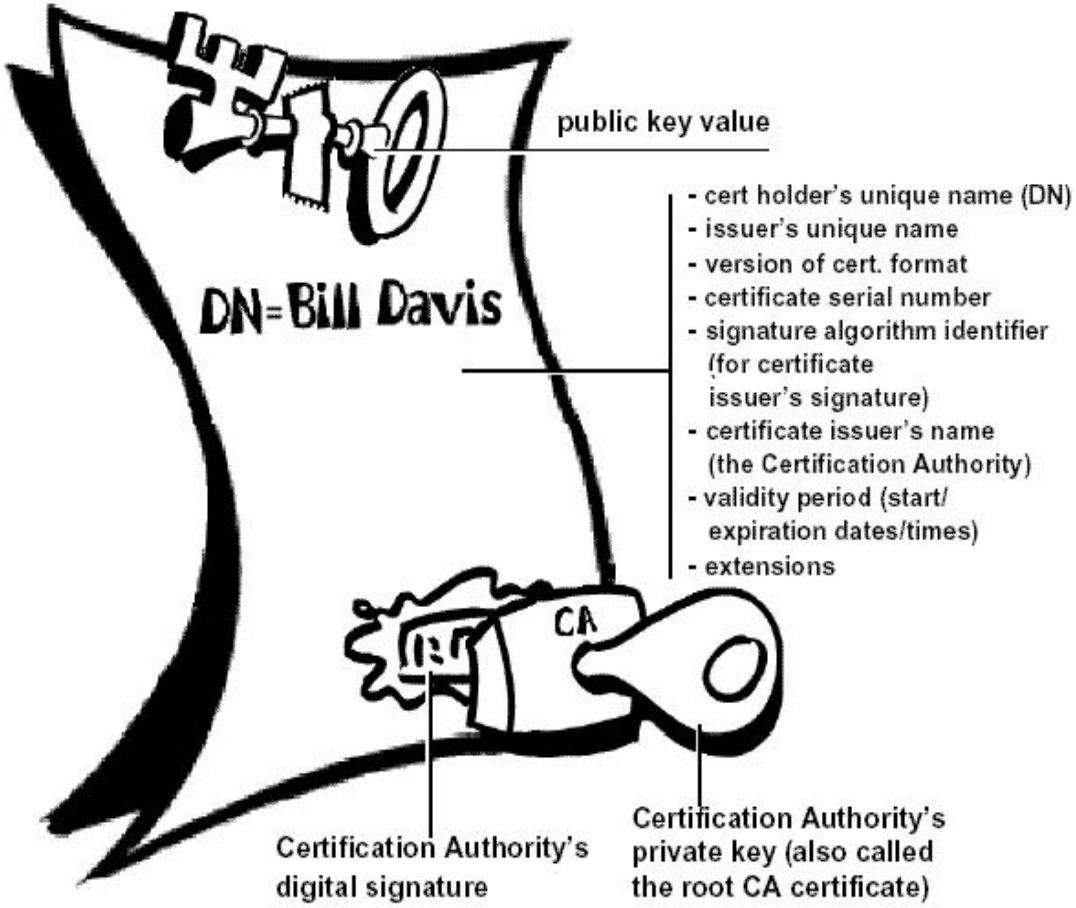


Figure 1-10. An X.509 certificate

نظام أمن جيد يعتمد على

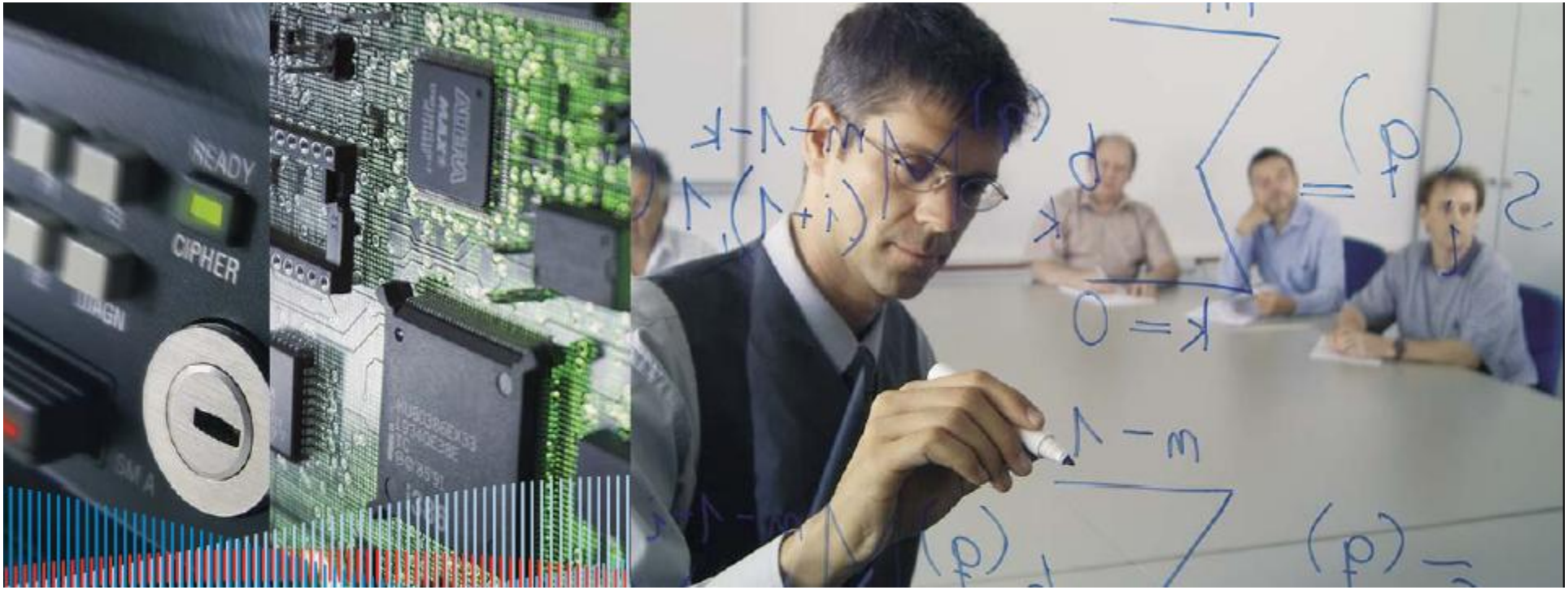
- التوقيع باستخدام مفتاحك الخاص private key
- التشفير باستخدام المفتاح العام لشريكك Public key
- استخدام مفاتيح تشفير طويلة (حتى نتفادى الاختراق)
  - مفتاح 40 بت => 2^{40} مفتاح = حوالي 10^{12} ، مثلا كل اختبار يحتاج 1 ميكرو ثانية => جميع الحالات تحتاج 35 سنة ! ولكن مع 35 حاسب سنحتاج لعام واحد!
  - مفتاح 128 بت => $3.4*10^{38}$ مفتاح ، نفس الحالة السابقة بحاسب واحد نحتاج 10^{27} سنة

المخاطر Threats

- مفاتيح التشفير موجودة في الحاسب
- دائما يوجد من يتعقب ويتتبع ما يوجد على حاسبنا

دراسة حالة: تنصت على لوحة المفاتيح

- نفترض أن حاسبنا قد تم اختراقه من قبل Virus غير معروف أو أن أحد الاشخاص الذين يشاركوننا بالحاسب قد دس لنا برنامج تنصت دون علمنا.
- يقوم هذا البرنامج بالتنصت على كل ما يتم إدخاله على لوحة المفاتيح وخاصة كلمات السر مثل البريد إلكتروني وأرقام Visa - MasterCard ثم يخزنها بملف ويرسلها بالبريد الإلكتروني للشخص الدخيل.



How AdvIT can improve the security

الحل لحماية مفاتيح التشفير وكلمات السر هو باستخدام:

key : Smart Keys & Cards

- هي عبارة عن جهاز شخصي محمول يمثلك على شبكة ما
- مثال:
  - smart cardsالبطاقات الذكية
  - biometrics: fingerprint readers قارئات البصمة
  - USB keys

- إن استخدام هذه الأجهزة يمكننا من الحفاظ على مفاتيحنا السرية بعيداً عن الحواسب والشبكات الغير حصينة

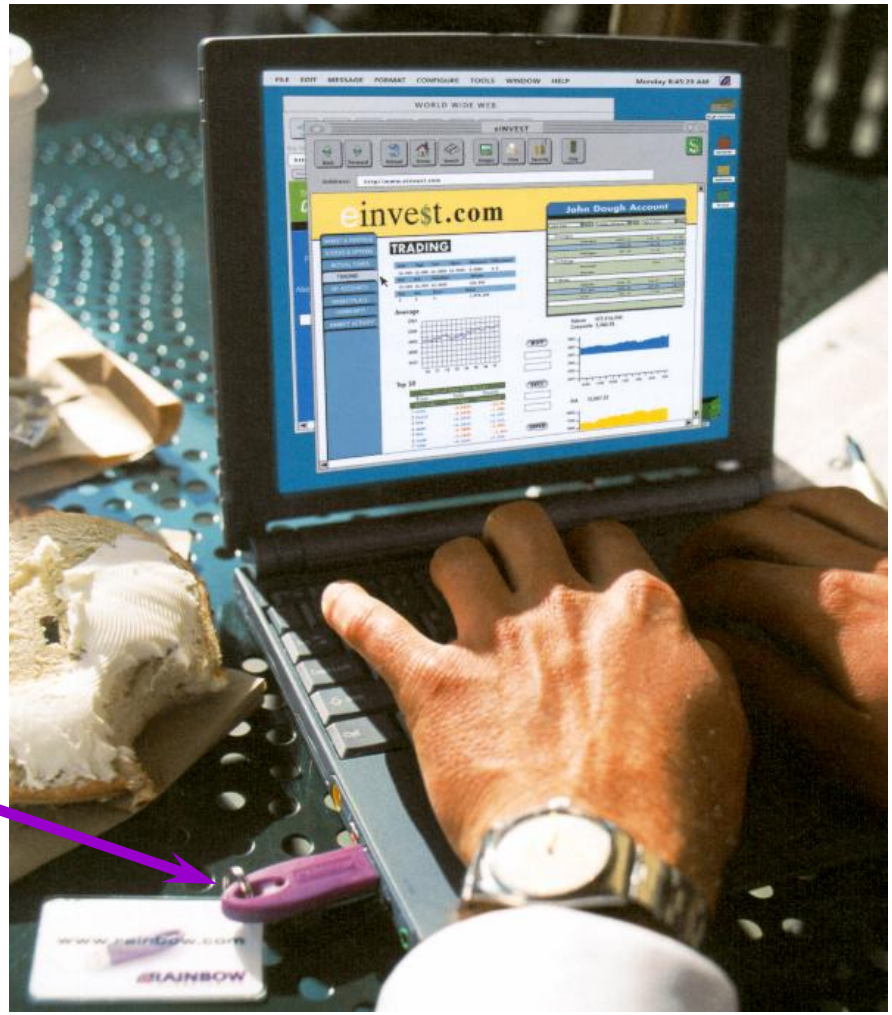
Token form factors

	Passwords	**PW Generator**	**Smartcard**	**USB key**	***Biometric***
Network Security	Poor	Good	Excellent	Excellent	Poor
Stores data	No	No	Limited	Yes	No
Easy to manage	No	No	Yes	Yes	No
Convenient	No	No	Yes	Yes	Yes
Readerless	Yes	Yes	No	Yes	No
Cost	Low	High	Medium	Medium	High
Also a card	No	No	Yes	No	No

What is SmartToken?

- ***Smart card and a Reader in a USB form factor***
- ***A family of full featured tokens providing strong authentication for end users.***
- ***A personal, portable, physical device representing you on a computer or network***

•USB: SmartKey



Advantages of using SmartKey الميزات

- Security أمن
- Portability قابلية النقل
- Ease of use for the end user سهولة الاستخدام

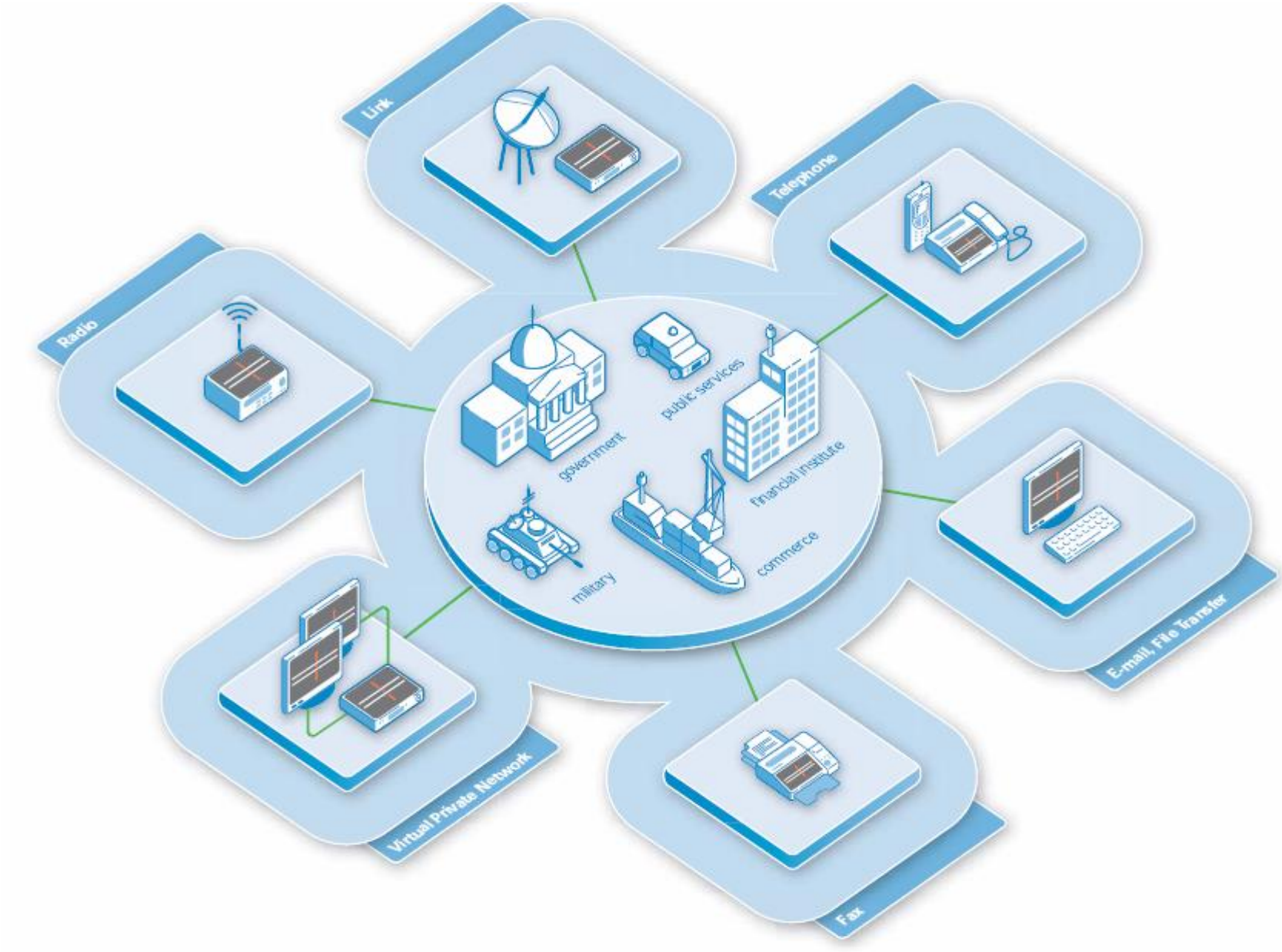
ميزات SmartKey في الأمن:

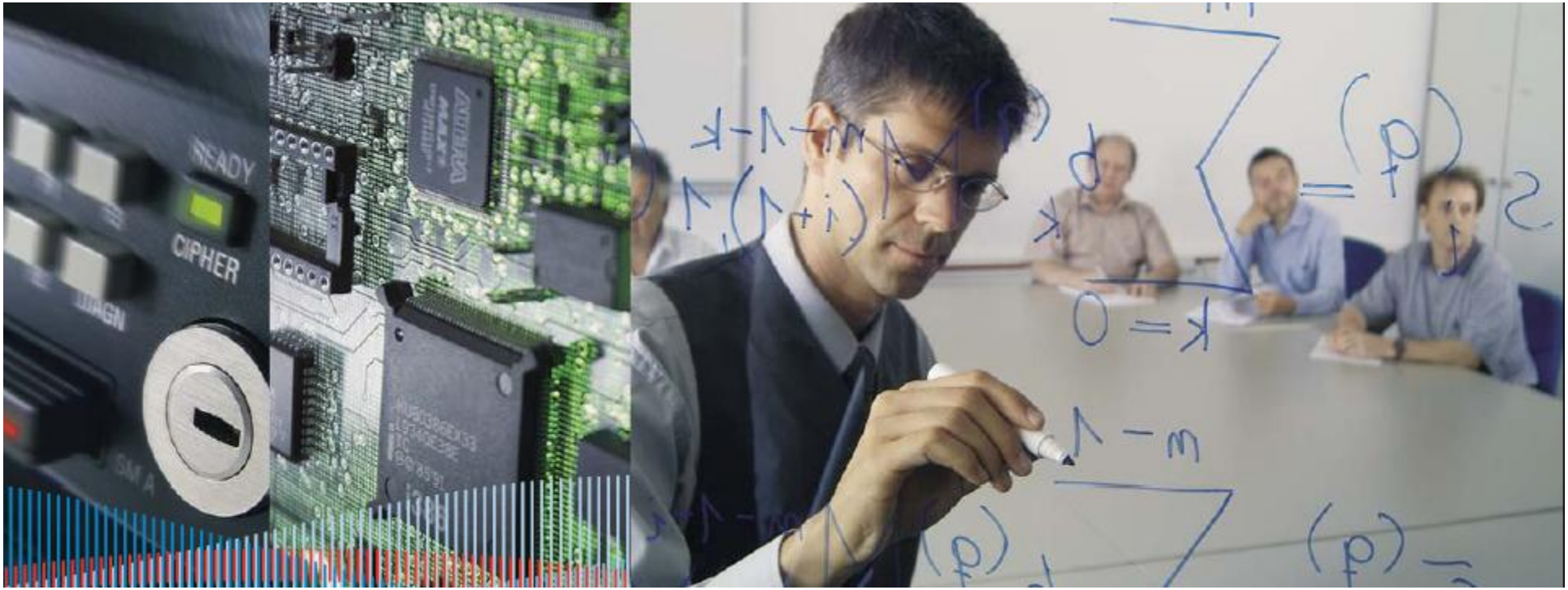
- On board key generation توليد داخلي لمفاتيح التشفير
- secure storage of private key حفظ آمن للمفاتيح الخاصة
- On board signing التوقيع الإلكتروني داخل المفتاح
- Access token with two factor authentication عاملان للاستيقان
  - what you know (login name, password) ما تعرف
  - what you have: iKey ما تملك

Token Applications تطبيقات

- Secure Email
- Secure web access
- VPN authentication
- Access control
- Laptop anti-theft
- Remote access
- Internet remote access
- PC Ignition key
- Parental controls
- Payments
- Form Signing
- Digital license holder
- PKI

Other Domains





Partners:

OmniSec, SwissCom, Phion, Avira, SafeBoot, Feitian,

omnisec

Keep Your Secrets Secret

Based in Neutral Switzerland

swisscom solutions

Swisscom Solutions AG
Risk & Security Consulting
Müllerstrasse 16
CH-8004 Zürich

Phone +41 58 222 80 44
Fax +41 58 222 88 55

eMail solutions@swisscom.com
Website www.swisscom.com/solutions

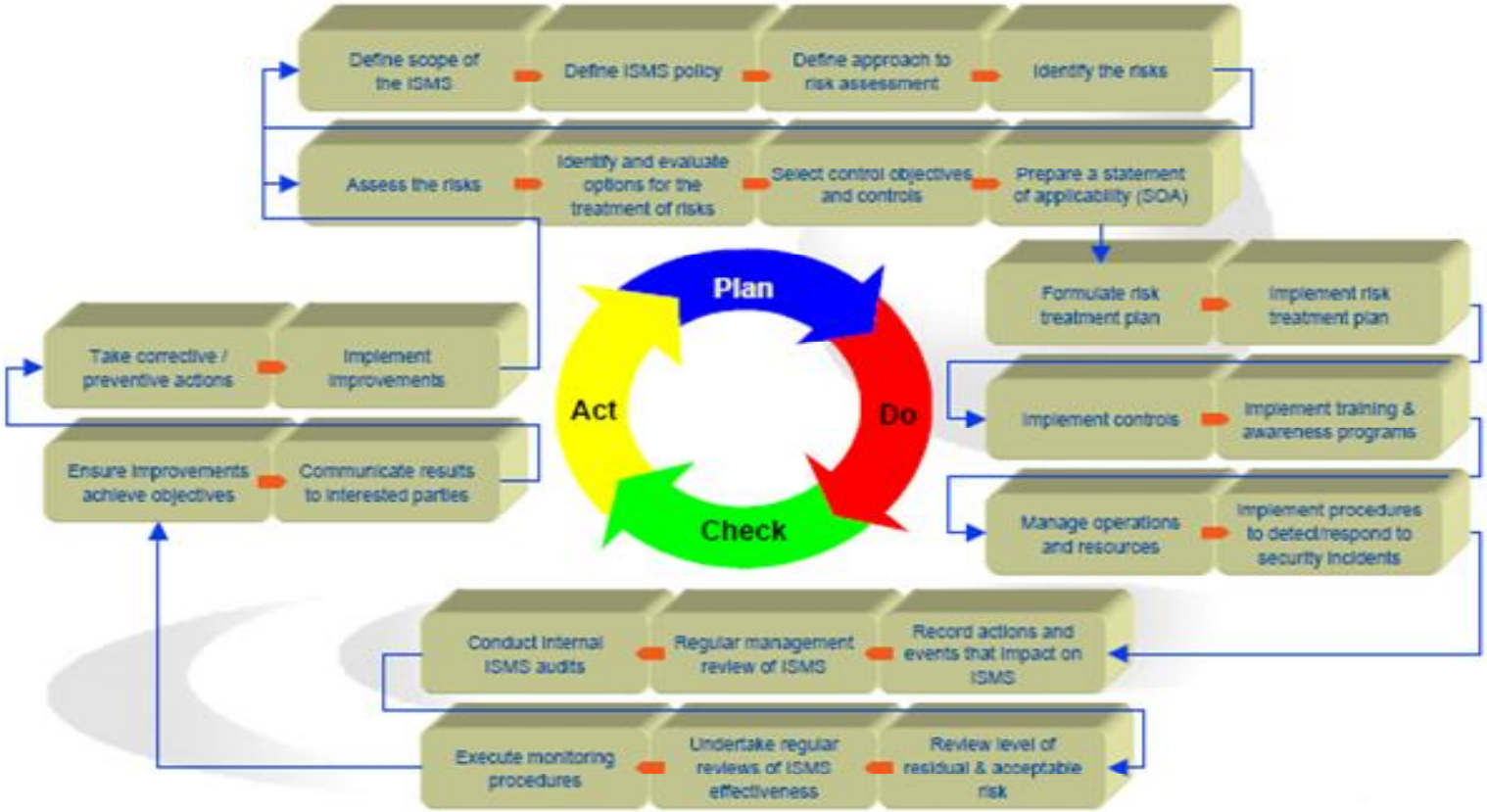
phion

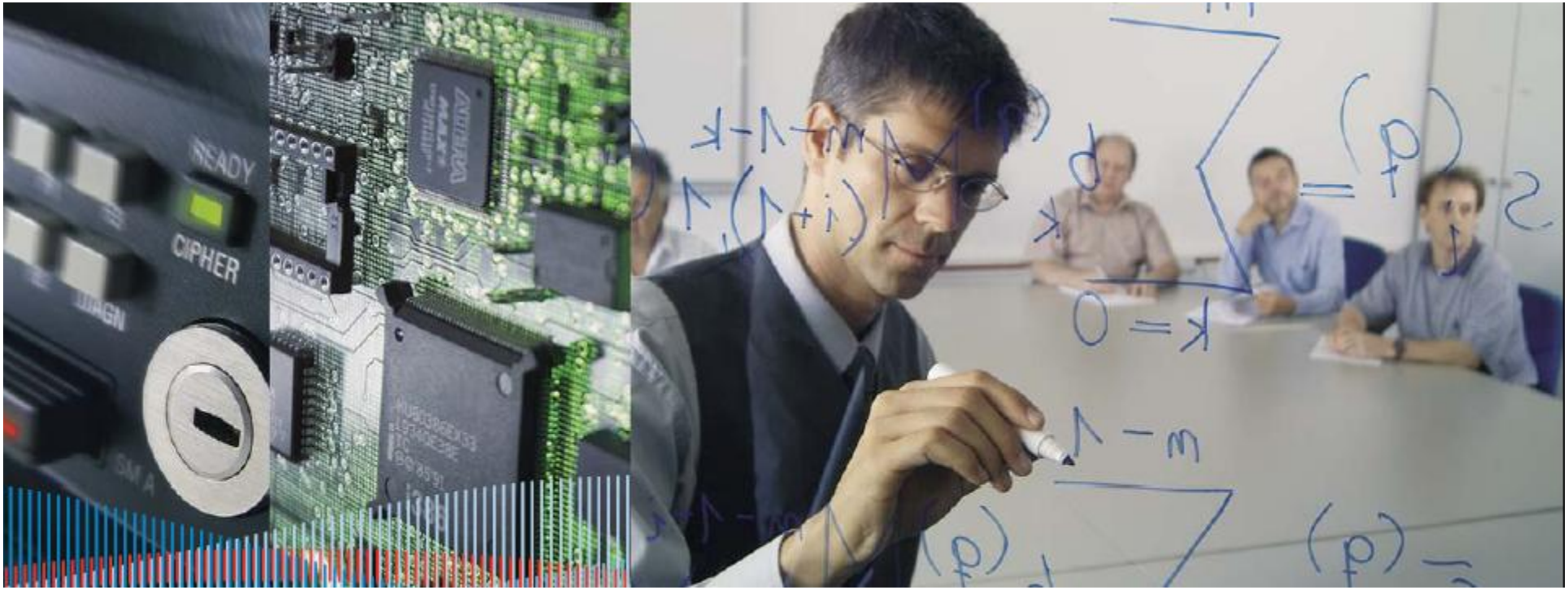
Not Only Products

- Hardware
- Software
- Consultancy & Test Penetration

Using international standards & Models

- Plan-Do-Check-Act (PDCA) Modells (ISO/IEC 27001)





Products:

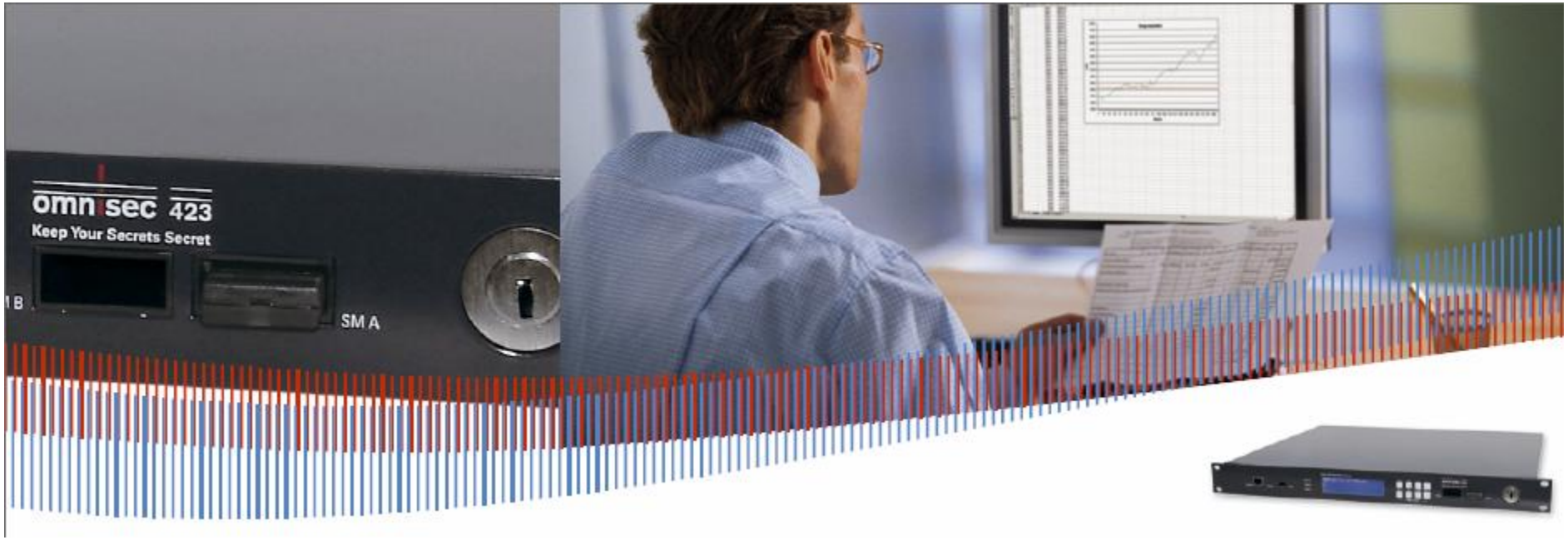
Telephone Encryptors

Fax Encryptors

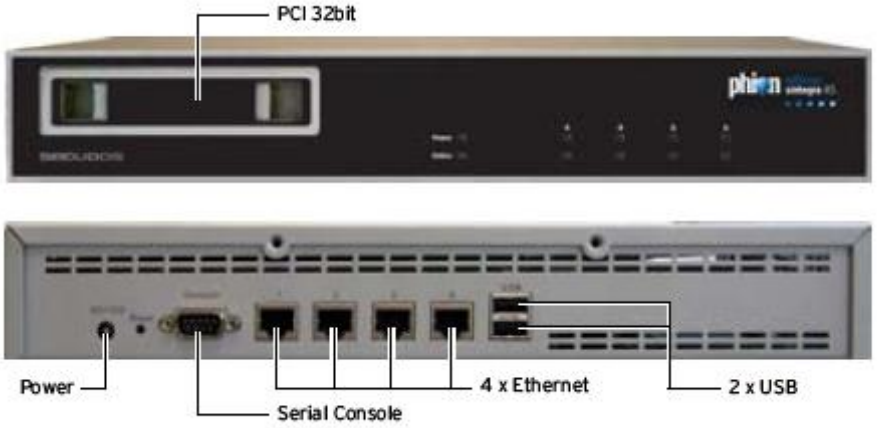
Radio Encryptors

Message & File Encryptors

IP Encryptors



Firewalls, IDS, IPS, Internet Security Gateway



phion netfence sintegra XS

phion netfence sintegra S