Cryptography – the Art of Secret Writing – From Old to New

Renate Scheidler

Centre for Information Security and Cryptography

Fields Institute, Toronto, November 18, 2006

What is Cryptography?

What is Cryptography?

κρυπτοζ – **hidden**

γραφειν – **to write**

What is Cryptography?

κρυπτοζ – **hidden**
γραφειν – **to write**

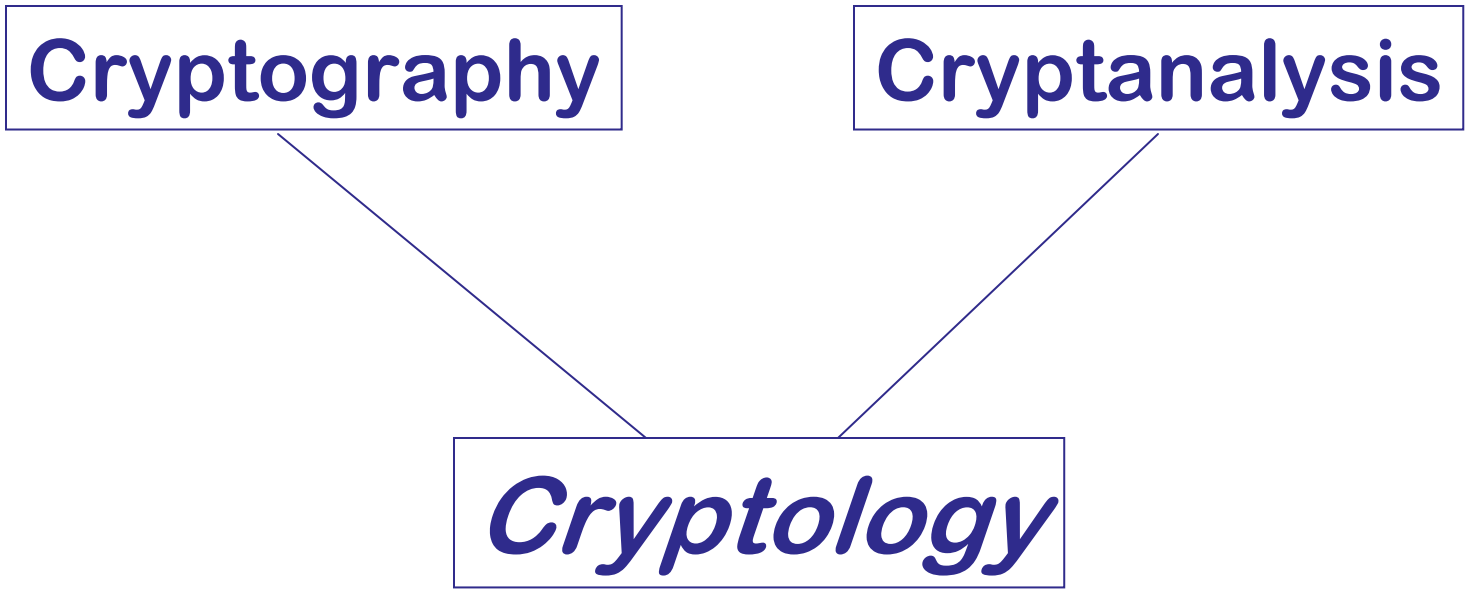
Encyclopedia Britannica online **defines it as**

"The practice of the enciphering and deciphering of messages in secret code in order to render them unintelligible to all but the intended receiver."

Cryptography

Cryptography

Cryptanalysis

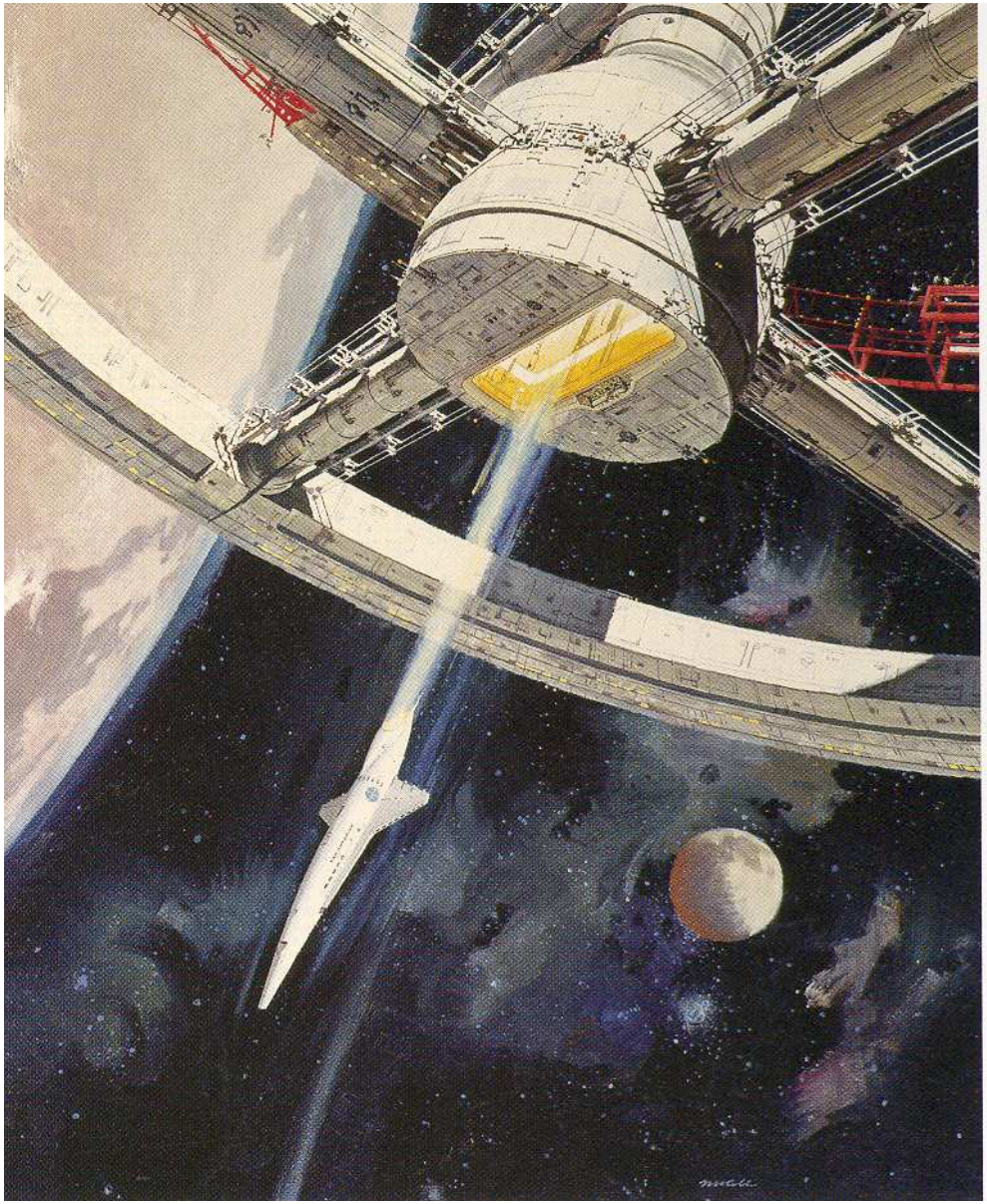

Cryptography
Cryptanalysis
Cryptology

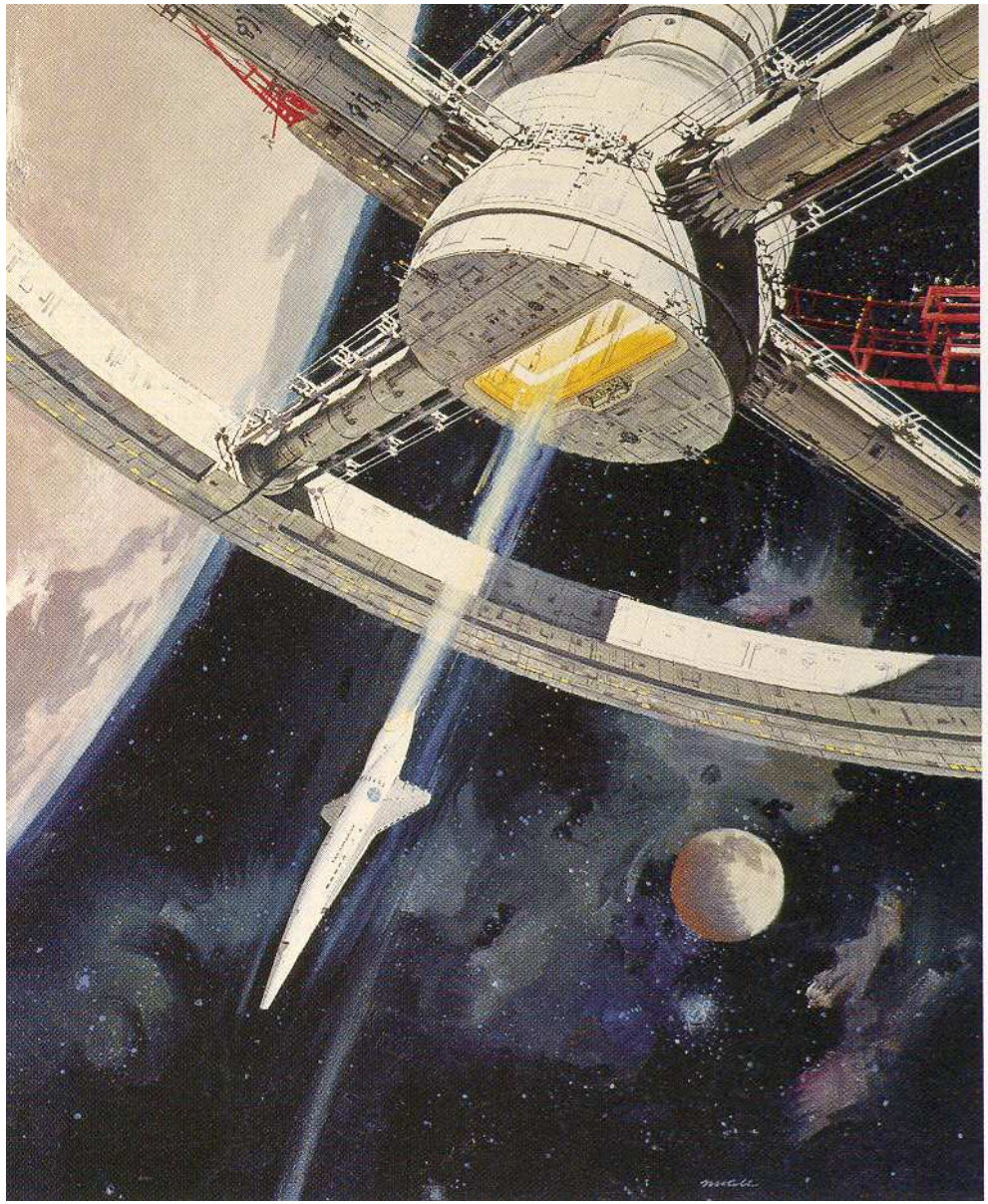
Conventional (One Key) Cryptosystem

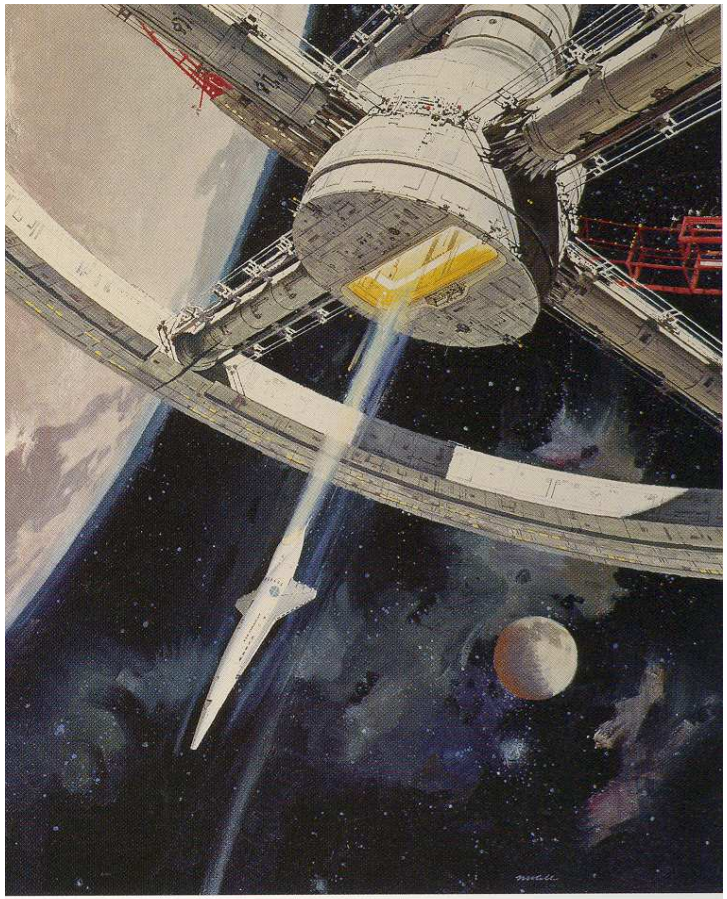
Example: *Shift Cipher*

Example: *Shift Cipher*

To encrypt, replace each letter in the plaintext by the letter ***K*** positions down the alphabet (with "wrap-around")







STANLEY KUBRICK'S

2001:

a space odyssey

Example: *Shift Cipher*

To encrypt, replace each letter in the plaintext by the letter K positions down the alphabet (with "wrap-around")

Eg, plaintext HAL $K = 1$

ciphertext

Example: *Shift Cipher*

To encrypt, replace each letter in the plaintext by the letter K positions down the alphabet (with "wrap-around")

Eg, plaintext HAL $K = 1$

ciphertext I

Example: *Shift Cipher*

To encrypt, replace each letter in the plaintext by the letter K positions down the alphabet (with "wrap-around")

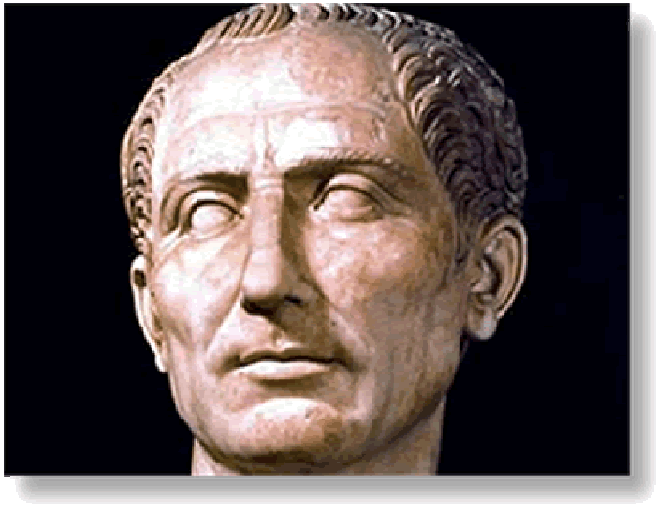
Eg, plaintext HAL $K = 1$
ciphertext IB

Example: *Shift Cipher*

To encrypt, replace each letter in the plaintext by the letter K positions down the alphabet (with "wrap-around")

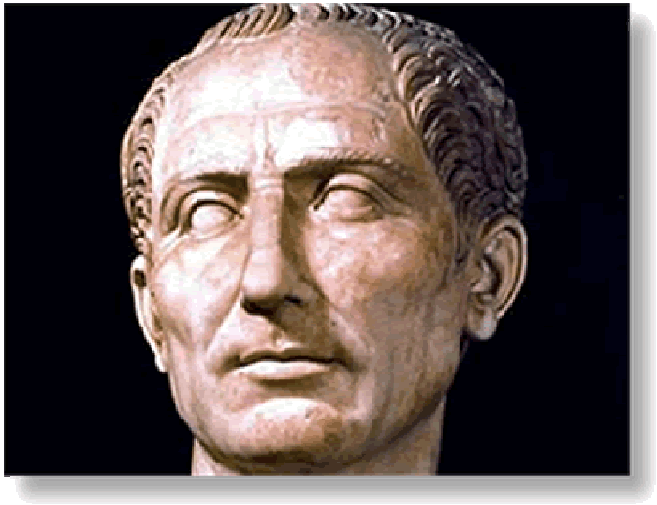
Eg, plaintext HAL $K = 1$
ciphertext IBM

According to Suetonius*,
Julius Caesar used this cipher with $K = 3$.



*_Lives of the Caesars_, Julius LVI, 110 CE).

According to **Suetonius***,
Julius Caesar used this cipher with $K = 3$.



******Lives of the Caesars*, Julius LVI, 110 CE).

This particular cipher is therefore sometimes called Caesar Cipher.

Most historic ciphers are of two types:

Most historic ciphers are of two types:

- **Substitution cipher** - replace every letter by another letter

Most historic ciphers are of two types:

- **Substitution cipher** - replace every letter by another letter
- **Transposition cipher** – permute the letters

Most historic ciphers are of two types:

- **Substitution cipher** - replace every letter by another letter
- **Transposition cipher** – permute the letters

Such ciphers can be broken with modern computers using statistical methods.

Most historic ciphers are of two types:

- **Substitution cipher** - replace every letter by another letter
- **Transposition cipher** – permute the letters

Such ciphers can be broken with modern computers using statistical methods.

Modern ciphers are *combinations* of the two types (*C. Shannon*, 1949)

Enigma

Enigma

Designed by A. Scherbius in the 1920s.

Enigma

Designed by A. Scherbius in the 1920s.
Used extensively by Germany in WW II.

Enigma

Designed by A. Scherbius in the 1920s.
Used extensively by Germany in WW II.

Enigma

Designed by A. Scherbius in the 1920s. Used extensively by Germany in WW II.

Enigma

Broken by M. Rejewski, H. Zygalski, and J. Rózyski in the 1930's.

Enigma

M. Rejewski

Broken by M. Rejewski,
H. Zygalski, and
J. Rózyski in the 1930's.

More instrumental code breaking efforts in Great Britain in the 1930s by A. Turing.

Modern Ciphers

Modern Ciphers

- ***Data Encryption Standard*** **(DES)**
  NIST (NBS) 1977
  $2^{56} \approx 10^{17}$ keys
  Nowadays only used as 3-DES (triple encryption), NIST 1999

Modern Ciphers

- ***Data Encryption Standard*** **(DES)**
  NIST (NBS) 1977
  $2^{56} \approx 10^{17}$ keys
  Nowadays only used as 3-DES (triple encryption), NIST 1999

- ***Advanced Encryption Standard*** **(AES)**
  NIST 2001, recommended over 3-DES
  2^{128} or 2^{192} or 2^{256} keys

Modern Ciphers

- ***Data Encryption Standard*** **(DES)**
  NIST (NBS) 1977
  $2^{56} \approx 10^{17}$ keys
  Nowadays only used as 3-DES (triple encryption), NIST 1999

- ***Advanced Encryption Standard*** **(AES)**
  NIST 2001, recommended over 3-DES
  2^{128} or 2^{192} or 2^{256} keys

Estim. no. of particles in the universe: 2^{240}

Question: **How can the secret key be safely transmitted to the receiver?**

Question: How can the secret key be safely transmitted to the receiver?

Two Solutions:

Question: How can the secret key be safely transmitted to the receiver?

Two Solutions:

- **Public Key Cryptography**

Question: How can the secret key be safely transmitted to the receiver?

Two Solutions:

- Public Key Cryptography
- Key Establishment Protocols

Question: How can the secret key be safely transmitted to the receiver?

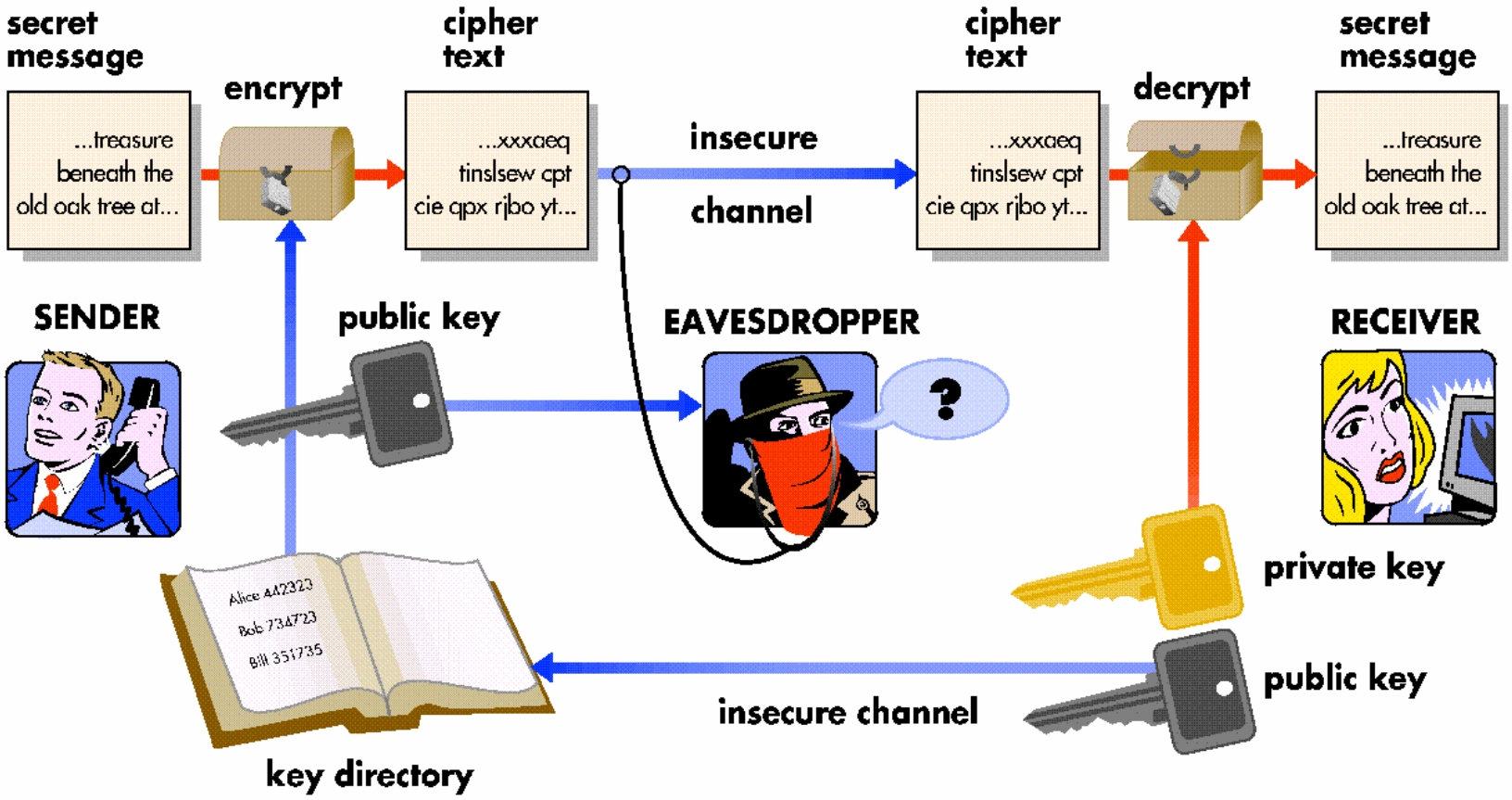
Two Solutions:

- **Public Key Cryptography**
- **Key Establishment Protocols**

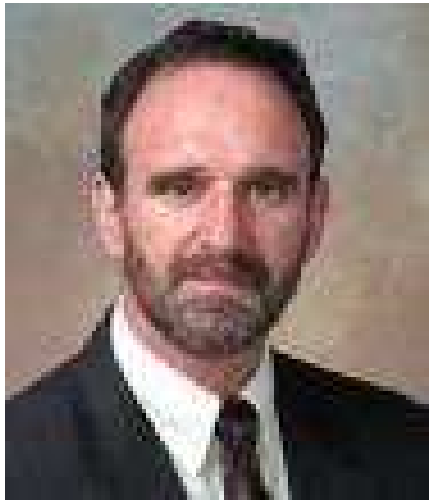
(W. Diffie & M. Hellman, 1976)

Public (Two) Key Cryptosystem

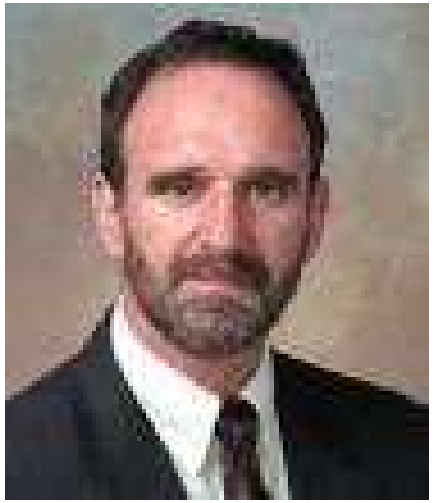
Public (Two) Key Cryptosystem



Officially, PKC was invented by W. Diffie and M. Hellman at Stanford University in 1976



Officially, PKC was invented by W. Diffie and M. Hellman at Stanford University in 1976



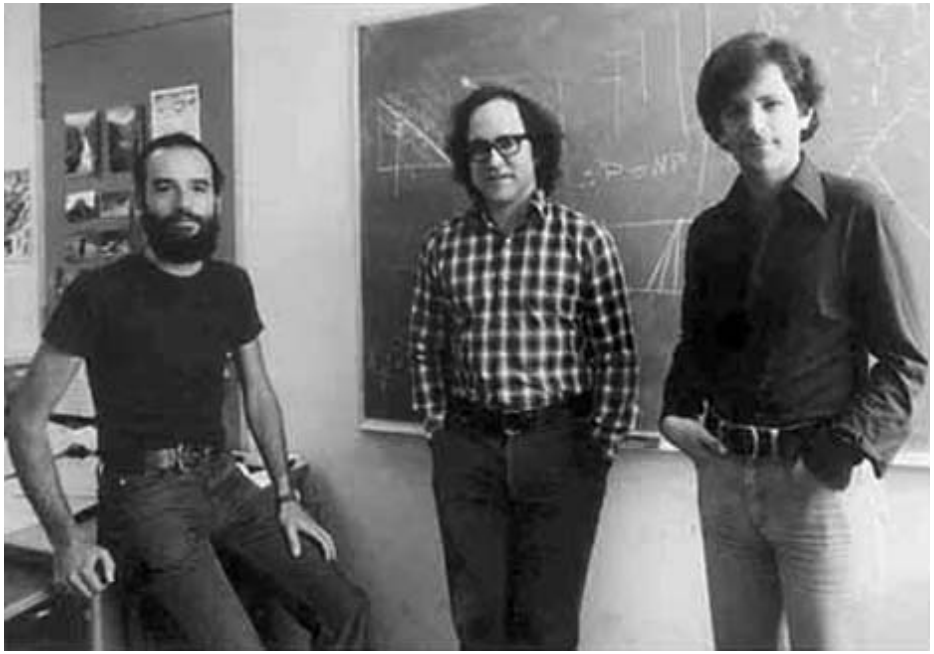
It was also invented (in secret) a few years earlier by J. Ellis at GCHQ Great Britain

- The **security** of public key systems and key establishment protocols is based on some **mathematical problem** that is widely believed (although frequently not *proven*) to be very **difficult**.

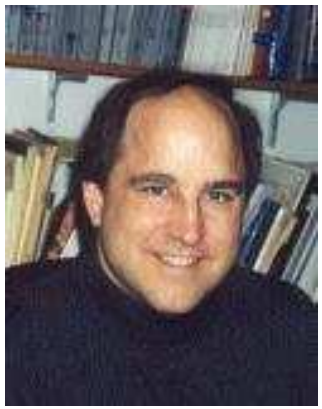
- The **security** of public key systems and key establishment protocols is based on some **mathematical problem** that is widely believed (although frequently not *proven*) to be very **difficult**.
- The idea is that an adversary needs to solve an instance of this difficult problem in order to **break** the system.

- The **security** of public key systems and key establishment protocols is based on some **mathematical problem** that is widely believed (although frequently not *proved*) to be very **difficult**.
- The idea is that an adversary needs to solve an instance of this difficult problem in order to **break** the system.
- Most of the time, the underlying problem stems from **number theory**.

The most widely used public key system is **RSA** (**R**ivest, **S**hamir, **A**dleman, 1978).

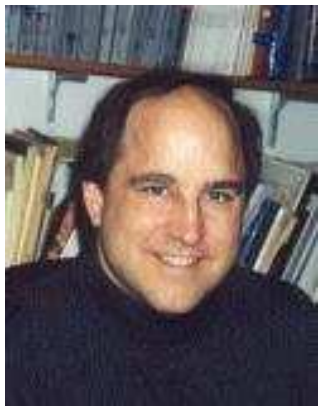


The most widely used public key system is **RSA** (**R**ivest, **S**hamir, **A**dleman, 1978).



RSA is based on the presumed difficulty of the **Integer Factorization Problem**: given an integer, find its **prime factors**.

The most widely used public key system is **RSA** (**R**ivest, **S**hamir, **A**dleman, 1978).



RSA is based on the presumed difficulty of the **Integer Factorization Problem**: given an integer, find its **prime factors**.

E.g. 787061080478274202283
= 56409643 x 13952598148481

Using a Public Key Cryptosystem:

Using a Public Key Cryptosystem:

- Each user has a *public key* **e** for encryption and a *private key* **d** for decryption.

Using a Public Key Cryptosystem:

- Each user has a *public key* **e** for encryption and a *private key* **d** for decryption.
- To send a confidential message **m** to **Alice**, **Bob** looks up **Alice**'s public key **e**, encrypts **m** with **e**, and send the ciphertext

$$c = E_e(m).$$

Using a Public Key Cryptosystem:

- Each user has a *public key* **e** for encryption and a *private key* **d** for decryption.
- To send a confidential message **m** to **Alice**, **Bob** looks up **Alice**'s public key **e**, encrypts **m** with **e**, and send the ciphertext

$$c = E_e(m).$$

- **Alice** then decrypts **c** with her private key **d** to obtain

$$D_d(c) = D_d(E_e(m)) = m.$$

Disadvantage of public key systems:

Disadvantage of public key systems:

- They unfortunately tend to be much slower than conventional crypto-systems, by a factor of 1000-1500.

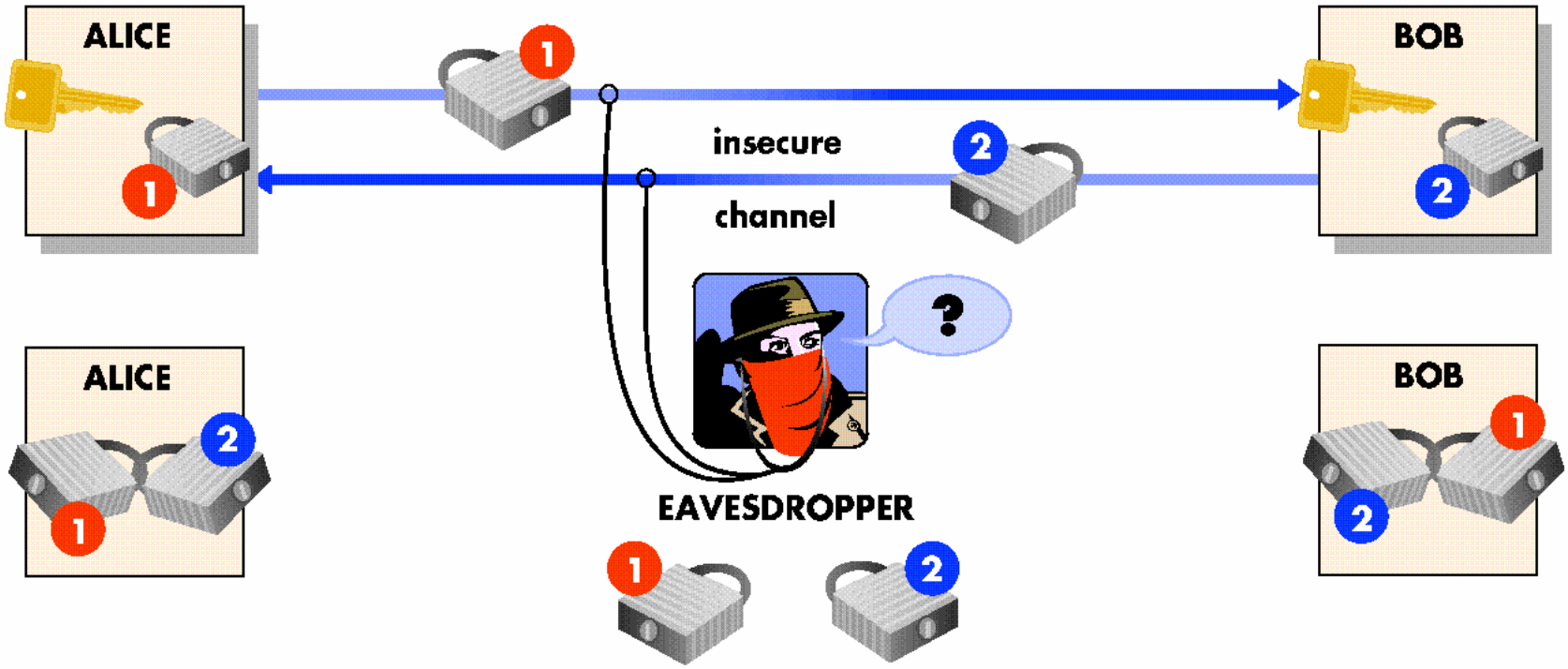
Disadvantage of public key systems:

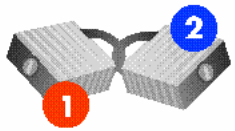
- They unfortunately tend to be much slower than conventional crypto-systems, by a factor of 1000-1500.

- In the context of encryption, they are therefore predominantly used for cryptographic key exchange, whereas bulk encryption is done with conventional systems, such as AES.

Key Establishment Protocol

Key Establishment Protocol





THE SECRET KEY IS: Two locks locked together.
Eavesdropper gets two locked locks & cannot open them.

The most widely used means for key establishment are:

The most widely used means for key establishment are:

- Public key cryptosystems

The most widely used means for key establishment are:

- Public key cryptosystems
- Diffie-Hellman Key Exchange Protocol (W. Diffie & M. Hellman, 1976).

The most widely used means for key establishment are:

- Public key cryptosystems
- Diffie-Hellman Key Exchange Protocol (W. Diffie & M. Hellman, 1976).
- Elliptic Curve Cryptography (ECC).

The most widely used means for key establishment are:

- Public key cryptosystems
- **Diffie-Hellman Key Exchange Protocol** (W. Diffie & M. Hellman, 1976).
- **Elliptic Curve Cryptography** (ECC).
- The security of DH and ECC is based on the presumed difficulty of the **Discrete Logarithm Problem** (DLP) for **finite fields** and **elliptic curves**, respectively.

What can modern cryptography do?

What can modern cryptography do?

- **Confidentiality** - keeping data secret from all but those authorized to see it.

What can modern cryptography do?

- **Confidentiality** - keeping data secret from all but those authorized to see it.
- **Data Integrity** - assuring that data has not been altered by unauthorized means.

What can modern cryptography do?

- **Confidentiality** - keeping data secret from all but those authorized to see it.
- **Data Integrity** - assuring that data has not been altered by unauthorized means.
- **Data-origin authentication** - corroborating the source of data.

What can modern cryptography do?

- **Confidentiality** - keeping data secret from all but those authorized to see it.
- **Data Integrity** - assuring that data has not been altered by unauthorized means.
- **Data-origin authentication** - corroborating the source of data.
- **Entity authentication** - corroborating the identity of an entity.

What can modern cryptography do?

- **Confidentiality** - keeping data secret from all but those authorized to see it.
- **Data Integrity** - assuring that data has not been altered by unauthorized means.
- **Data-origin authentication** - corroborating the source of data.
- **Entity authentication** - corroborating the identity of an entity.
- **Non-repudiation** - preventing an entity from denying previous commitments or actions.

Digital Signatures

Digital Signatures

- A means for **authentication** and **non-repudiation**.

Digital Signatures

- A means for **authentication** and **non-repudiation**.
- Realizable using public key cryptography.

Digital Signatures

- A means for **authentication** and **non-repudiation**
- Realizable using public key cryptography.
- To sign a message m, Alice "decrypts" m with her private key d to obtain $s = D_d(m)$ and send the pair (m, s) to Bob.

Digital Signatures

- A means for **authentication** and **non-repudiation**
- Realizable using public key cryptography.
- To sign a message m, Alice "decrypts" m with her private key d to obtain $s = D_d(m)$ and send the pair (m, s) to Bob.
- Bob looks up Alice's public key e and "encrypts" s with e to obtain

$$E_e(s) = E_e(D_d(m)) = m.$$

Digital Signature Systems in Use

Digital Signature Systems in Use

- **Digital Signature Algorithm (DSA)**
  NIST 2000

Digital Signature Systems in Use

- **Digital Signature Algorithm (DSA)**
  NIST 2000

- **RSA**, ANSI X9.31, 1998
  Financial Services Industry

Digital Signature Systems in Use

- **Digital Signature Algorithm (DSA)**
  NIST 2000

- **RSA**, ANSI X9.31, 1998
  Financial Services Industry

- **Elliptic Curve Digital Signature Algorithm (ECDSA)**, ANSI X9.62, 1998

Question: How does cryptography relate to information security?

Question: How does cryptography relate to information security?

We constantly read and hear about

- internet worms, viruses, Trojan horses
- defaced web sites
- hacked computers
- identity theft
- phishing
- war driving & war walking
- stolen credit card numbers …

"Mr. Grimshawe, somebody's hacked into the office computer!"

Question: How does cryptography relate to information security?

We constantly read and hear about

- internet worms, viruses, Trojan horses
- defaced web sites
- hacked computers
- identity theft
- phishing
- war driving & war walking
- stolen credit card numbers …

"Mr. Grimshawe, somebody's hacked into the office computer!"

Whose fault is it? Is cryptography to blame?

From Cryptography to Security

From Cryptography to Security

Cryptographic Primitive

From Cryptography to Security

Protocol

Cryptographic Primitive

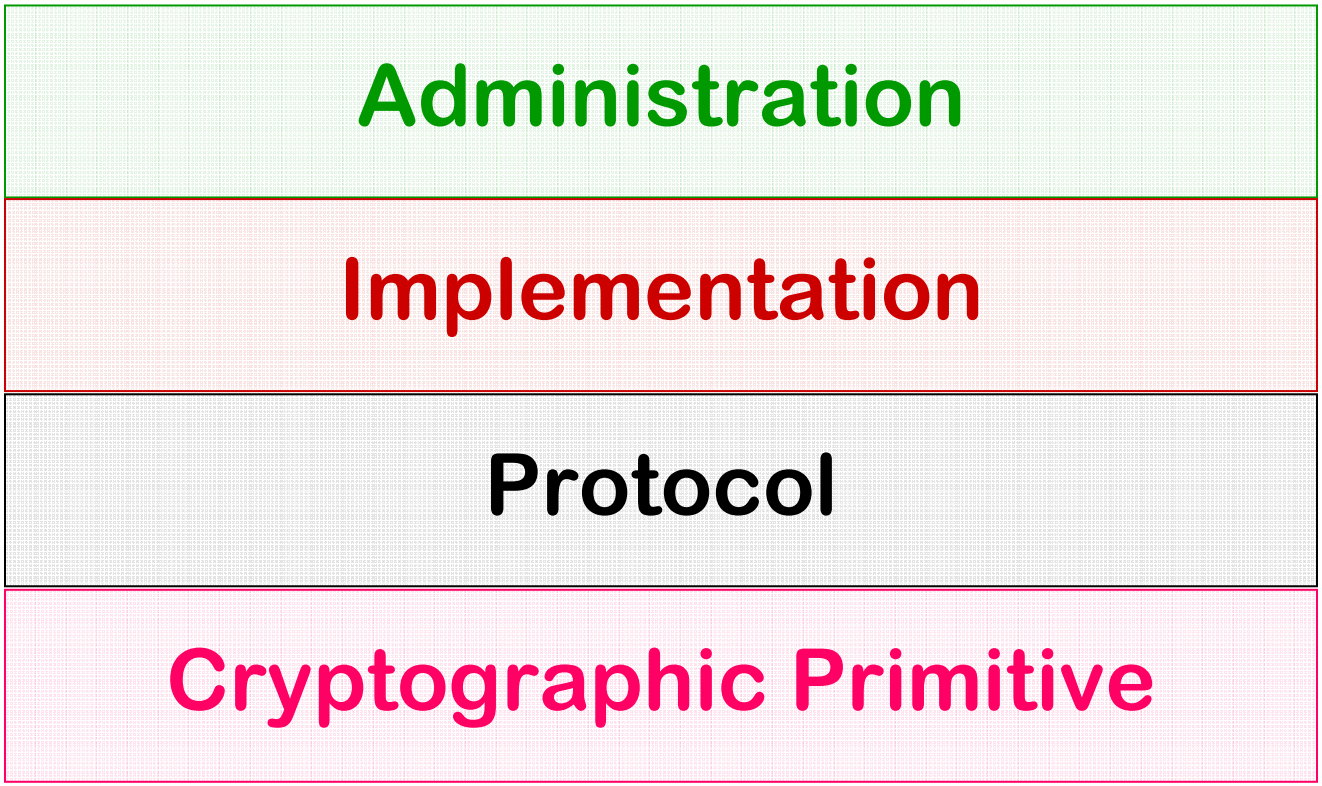
From Cryptography to Security

Implementation

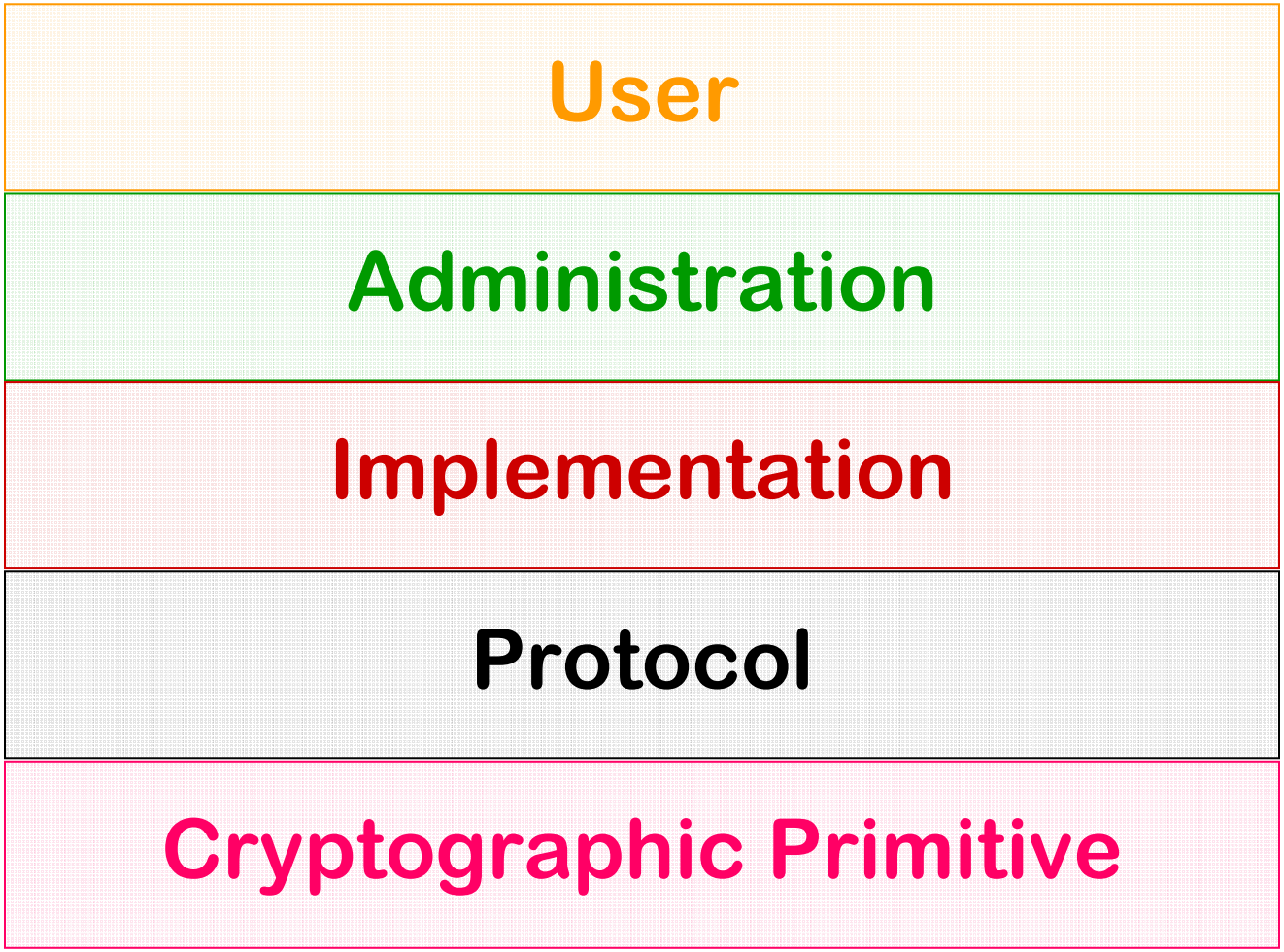
Protocol

Cryptographic Primitive

From Cryptography to Security



From Cryptography to Security



Cryptographic Primitive

SHA-1 – A recently broken cryptographic tool

SHA-1 – A recently broken cryptographic tool

- **SHA-1** (**S**ecure **H**ash **A**lgorithm **1**) is an example of a **hash function**.

SHA-1 – A recently broken cryptographic tool

- **SHA-1** (Secure Hash Algorithm 1) is an example of a **hash function**.
- **Hash functions** are used to prevent the forgery of digital signatures.

SHA-1 – A recently broken cryptographic tool

- **SHA-1** (Secure Hash Algorithm 1) is an example of a **hash function**.
- **Hash functions** are used to prevent the forgery of digital signatures.
- In February 2005, **X. Wang** and **H. Yu** of Shandong University China and **Y. L. Yin**, an independent security consultant in the US, found a collision in SHA-1 2000 times faster than exhaustive search.

From Cryptography to Security

Protocol

Cryptographic Primitive

Impersonation – An example of protocol failure

Impersonation – An example of protocol failure

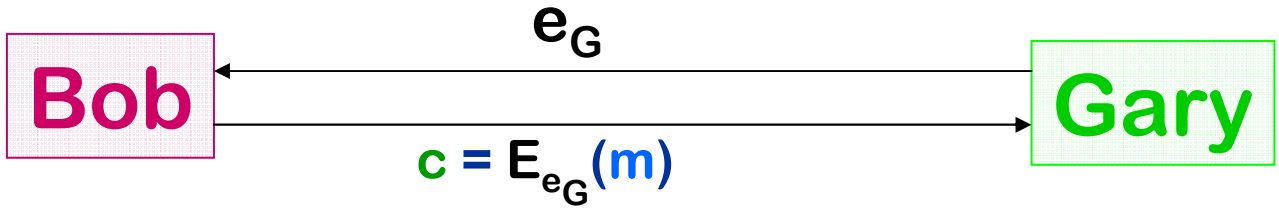
- Gary substitutes Alice's public key e_A by his own public key e_G.

Impersonation – An example of protocol failure

- Gary substitutes Alice's public key e_A by his own public key e_G.
- Bob now encrypts a message m to Alice with e_G, thinking it is e_A.

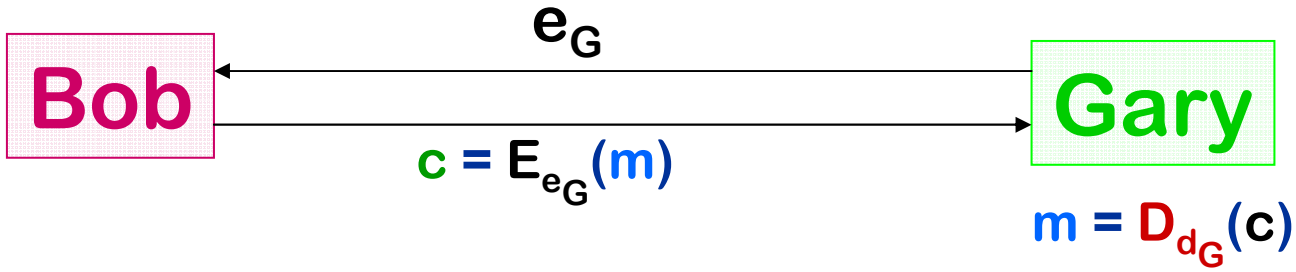
Impersonation – An example of protocol failure

- Gary substitutes Alice's public key e_A by his own public key e_G.
- Bob now encrypts a message m to Alice with e_G, thinking it is e_A.
- Gary intercepts Bob's ciphertext c …



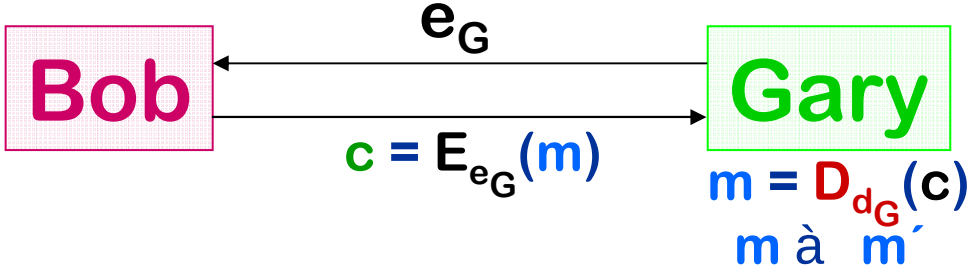
Impersonation – An example of protocol failure

- Gary substitutes Alice's public key e_A by his own public key e_G.
- Bob now encrypts a message m to Alice with e_G, thinking it is e_A.
- Gary intercepts Bob's ciphertext c … and decrypts it.



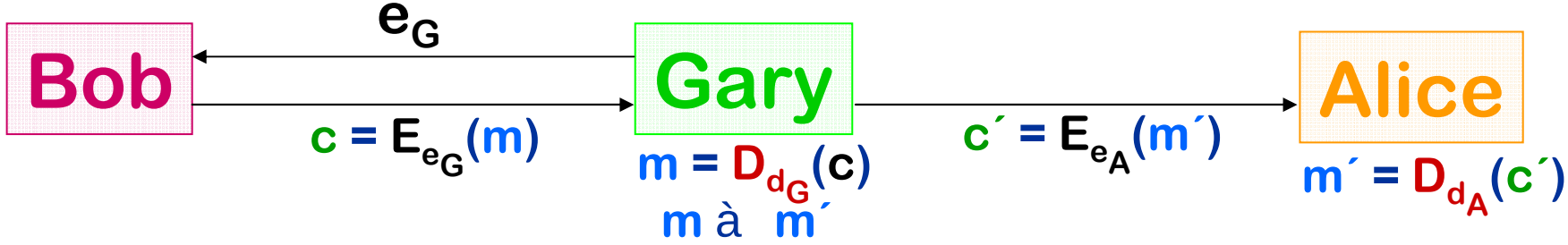
Impersonation – An example of protocol failure

- Even worse: Gary replaces Bob's message m by his own message m´.



Impersonation – An example of protocol failure

- Even worse: Gary replaces Bob's message m by his own message m´.
- He then encrypts m´ using Alice's public key e_A and sends the resulting ciphertext c´ to Alice.



From Cryptography to Security

Implementation

Protocol

Cryptographic Primitive

Predictable Keys – An example of implementation failure

Predictable Keys – An example of implementation failure

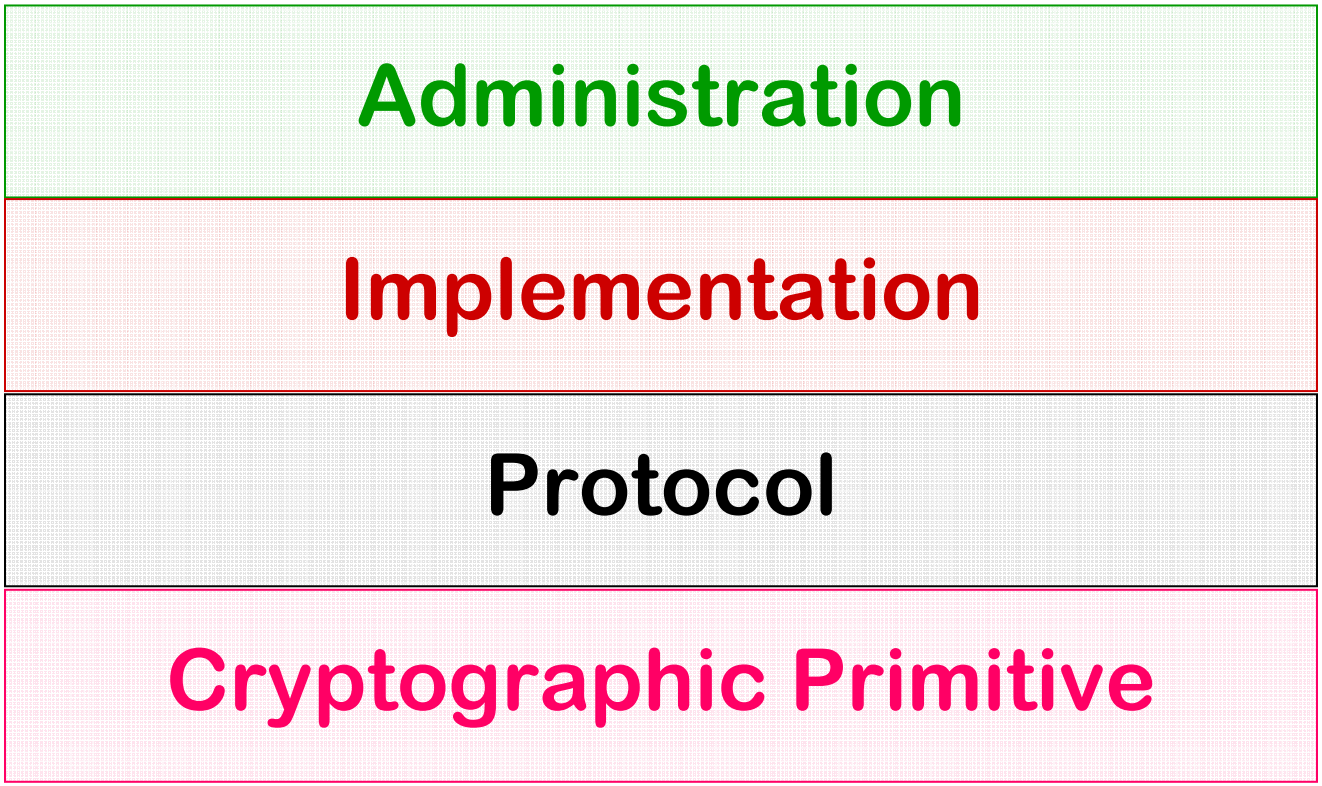
- Instead of generating a key randomly, predictable information (such as the date or the machine's IP address) is incorporated in the key generation.

Predictable Keys – An example of implementation failure

- Instead of generating a key randomly, predictable information (such as the date or the machine's IP address) is incorporated in the key generation.

- When using a pseudo-random bit generator, the program fails to start with a new seed each time.

From Cryptography to Security



Examples of administrative failure:

Examples of administrative failure:

Failure to install:

Examples of administrative failure:

Failure to install:

- system patches and upgrades

Examples of administrative failure:

Failure to install:

- system patches and upgrades
- anti-virus software and its upgrades

Examples of administrative failure:

Failure to install:

- system patches and upgrades
- anti-virus software and its upgrades
- network upgrades

Examples of administrative failure:

Failure to install:

- system patches and upgrades
- anti-virus software and its upgrades
- network upgrades
- firewalls

Examples of administrative failure:

Failure to install:

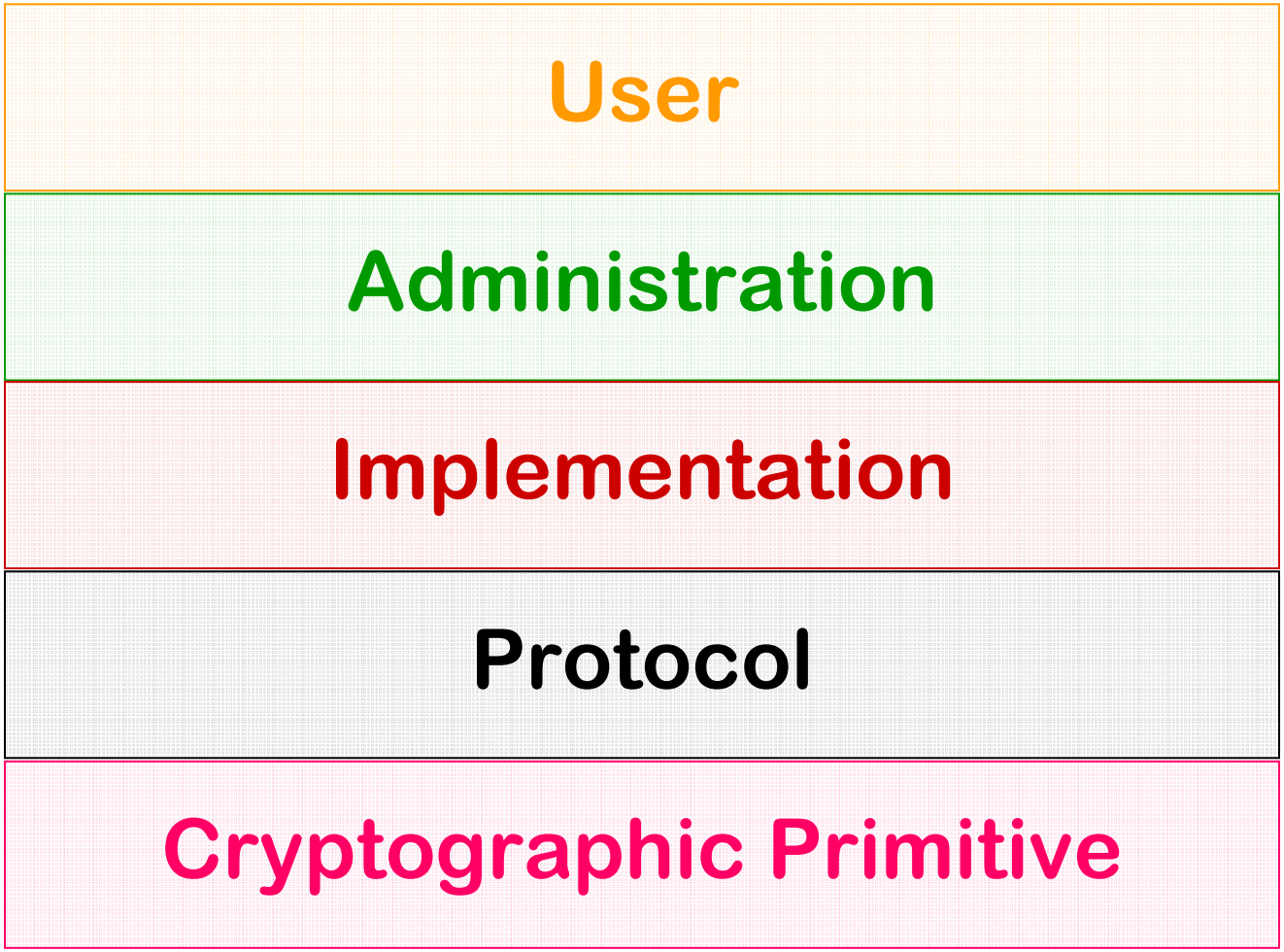
- system patches and upgrades
- anti-virus software and its upgrades
- network upgrades
- firewalls
- encryption software

Examples of administrative failure:

Failure to install:

- system patches and upgrades
- anti-virus software and its upgrades
- network upgrades
- firewalls
- encryption software
- physical security

From Cryptography to Security



Examples of user failure:

Examples of user failure:

- improper administration of personal computers

Examples of user failure:

- improper administration of personal computers
- bad choices for (or no) passwords

Examples of user failure:

- improper administration of personal computers
- bad choices for (or no) passwords
- using the same password for different systems and for too long a time

Examples of user failure:

- improper administration of personal computers
- bad choices for (or no) passwords
- using the same password for different systems and for too long a time
- sharing of passwords

Examples of user failure:

- improper administration of personal computers
- bad choices for (or no) passwords
- using the same password for different systems and for too long a time
- sharing of passwords
- easy access to computer (physical or other)

Examples of user failure:

- improper administration of personal computers
- bad choices for (or no) passwords
- using the same password for different systems and for too long a time
- sharing of passwords
- easy access to computer (physical or other)
- carelessness with personal records and mail (buy a shredder!)

A Fact:

A Fact:

Data from 2004:

Losses to US companies incurred through viruses, unauthorized access, and theft of proprietary information: US $105 million.

A Fact:

Data from 2004:

Losses to US companies incurred through viruses, unauthorized access, and theft of proprietary information: US $105 million.

Increase in losses from previous year due t
- **theft of proprietary information: 211%**

A Fact:

Data from 2004:

Losses to US companies incurred through viruses, unauthorized access, and theft of proprietary information: US $105 million.

Increase in losses from previous year due t

- **theft of proprietary information: 211%**
- **unauthorized access: 588%**

A Fact:

Data from 2004:

Losses to US companies incurred through viruses, unauthorized access, and theft of proprietary information: US$105 million.

Increase in losses from previous year due t

- **theft of proprietary information: 211%**
- **unauthorized access: 588%**

CSI/FBI Survey 2005, www.gocsi.com

And what about all this quantum stuff that everyone talks about?

And what about all this quantum stuff that everyone talks about?

- **Quantum cryptography** develops cryptographic systems whose security is based on the **laws of nature** rather than hard mathematical problems.

And what about all this quantum stuff that everyone talks about?

- **Quantum cryptography** develops cryptographic systems whose security is based on the **laws of nature** rather than hard mathematical problems.
- **Quantum information science** designs techniques for breaking traditional public key cryptosystems. A **quantum computer** would break every single public key cryptosystem currently in use.

Recreational Reading

- **David Kahn**, ***The Code Breakers***
  History up to World War II – a real classic, originally appeared in 1967
- **Simon Singh**, ***The Code Book*** **- The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography**
  Doubleday 1999
  www.simonsingh.net
- **Neal Stephenson**, ***Cryptonomicon***
  Avon Books 1999 – a novel