Introduction to Cryptology

Eric Filiol – ffiliol@gmail.com

28/10/2013

Agenda

- Introduction
- Basic Terminology
- The History of Cryptology
- Cryptology : Threats and Solutions :
  - Encryption
  - Hash
  - Electronic signature
- Basic Knowledge on Cryptanalysis
- Conclusion

Agenda

- Introduction
- Basic Terminology
- The History of Cryptology
- Cryptology : Threats and Solutions :
  - Encryption
  - Hash
  - Electronic signature
- Basic Knowledge on Cryptanalysis
- Conclusion

Introduction

CRYPTOLOGY = The science of secret

- Cryptology is underlying all other aspects of security
  - Who master cryptology masters everything else!
- One must protect oneself
  - Against what?
  - Against who?
  - How?

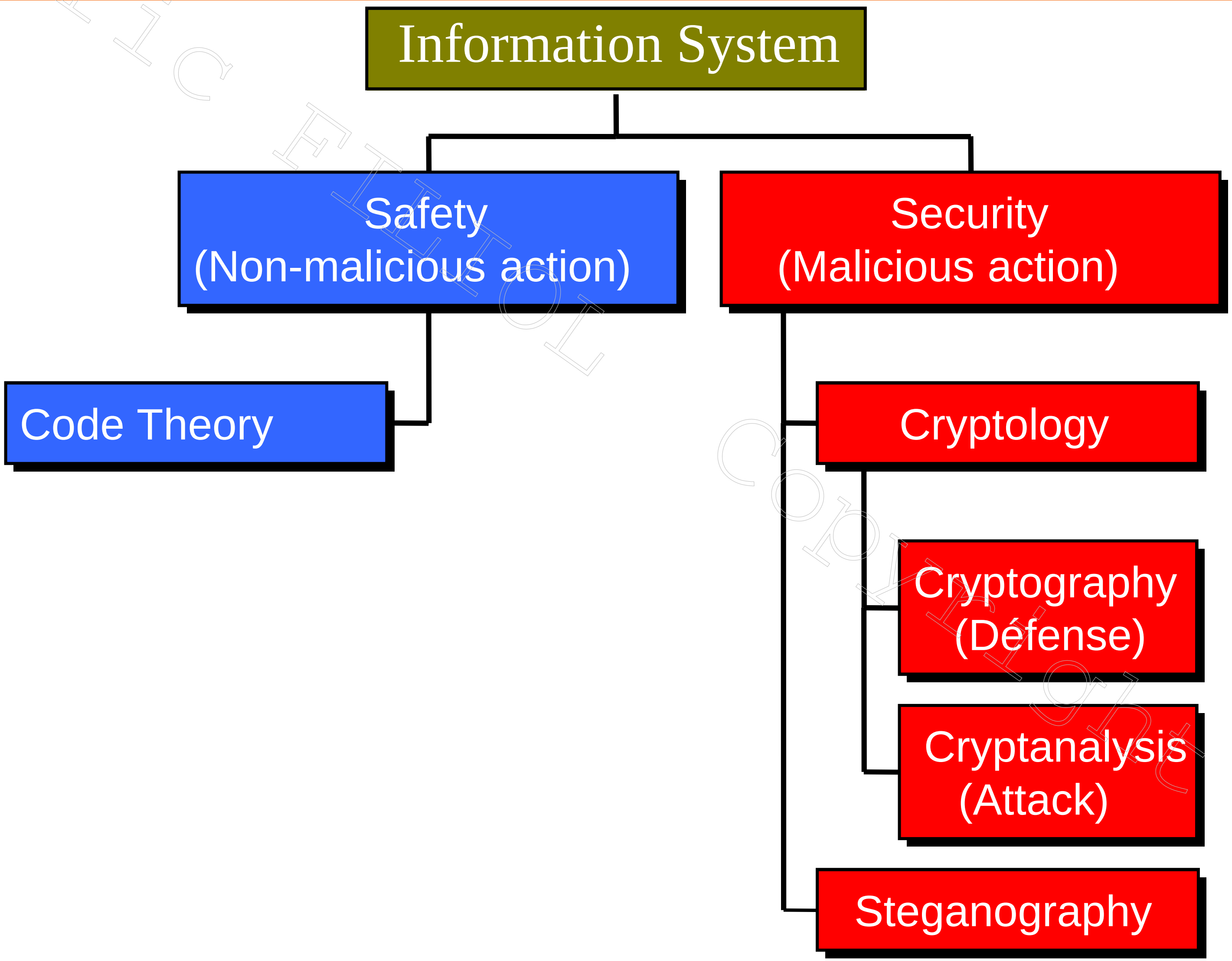
➔The threat must be analysed

Basic and general principle of security

Agenda

- Introduction
- Basic Terminology
- The History of Cryptology
- Cryptology : Threats and Solutions :
  - Encryption
  - Hash
  - Electronic signature
- Basic Knowledge on Cryptanalysis
- Conclusion

Basic Terminology



Basic Terminology

- **SAFETY :**

  The part of the ISS dedicated to the protection against non-malicious attacks upon information infrastructure (noise, CD scratch, breakdowns…)

  Example : error correcting code, parity check

- **SECURITY :**

  The part of the ISS dedicated to the protection against malicious attacks upon information itself (confidentiality, integrity…)

  Example : communication encryption, electronic signature

Basic terminology

- CODE : convention designed to be broadcast as <u>broadly as possible</u>.
  - Public convention ⇒ no secret
  - Example : Baudot Code, Morse code, ascii code,…

- CIPHER: convention designed to be broadcast <u>as little as possible</u>.
  - Secret convention ⇒ either the KEY or the KEYS

Basic Terminology

- **ENCRYPTION:**

  The process of converting plaintext into ciphertext using one or several secret elements (keys)

- **DECRYPTION :**

  The process of converting ciphertext back into plaintext using in a legitimate way using keys that may be different from those used during the encryption.

  - This definition explicits the difference between symmetric cryptography and asymmetric cryptography.

Basic Terminology

- CIPHERTEXT:

  Ouput of the encryption of a plaintext, also called cryptogramm (the encrypted ouput).

- KEY :

  Basic secret parameter which intervenes in the encryption or decryption process of the information. The system security is mainly based on the key.

Basic Terminology

- **SUBSTITUTION :**

  Letters of the plaintext are replaced with other letters. The statistical distribution of letters are permuted.

- **TRANSPOSITION :**

  Letters of the plaintext remain unchanged but the respective positions are modified. The statistical distribution is unchanged.

Basic Terminology

- SYMMETRIC ENCRYPTION:

  The single key is used for both encryption and decryption.

- ASYMMETRIC ENCRYPTION :

  Two keys are used: one for encryption and the other for decryption.

- HYBRID ENCRYPTION:

  Symmetric and asymmetric encryption are mixed and combined

- CRYPTOSYSTEM:

  The system includes an encryption algorithm, a decryption algorithm, the plaintext, the cyphertext, the key.

Basic Terminology

- **CRYPTANALYSIS :**

  This is the process and mathematical techniques which consist to break the cryptosystem in an illegitimate way in order to recover the secret key(s), or the plaintext, or both from the ciphertext, with or without the knowledge of the algorithm.

- **APPLIED CRYPTANALYSIS :**

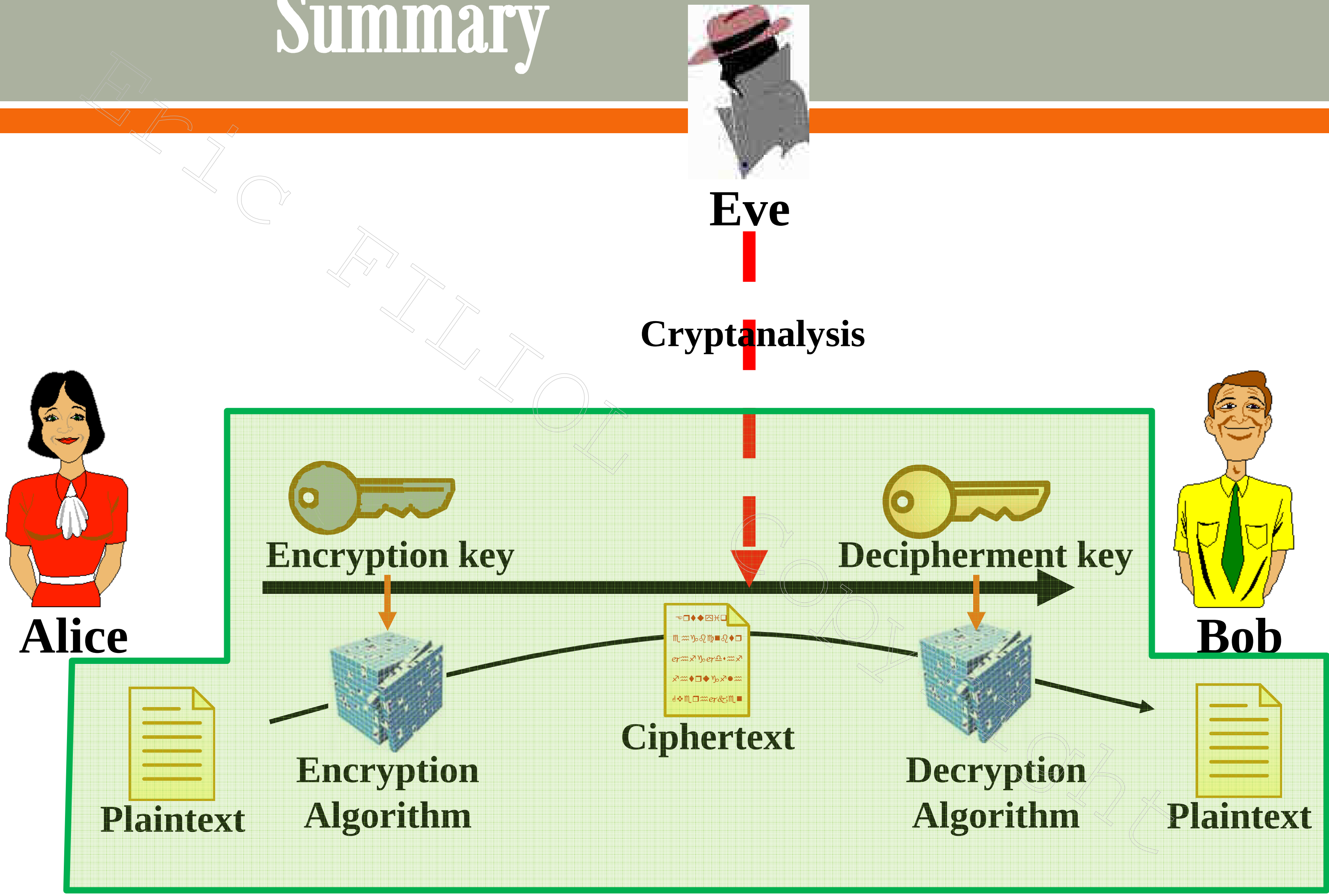
  Same goal but the techniques target either implemenation or maganement weaknesses instead of the mathematical properties of the algorithm.

  - The armoured door on paper wall syndrom
  - Malware
  - Side-channel attacks
  - Fault injection and tampering
  - Human intelligence
  - ...

Cryptology : the Actors

- One or more SENDERS (called A or Alice).
- One or more RECEIVERS (called B or Bob).
- A channel or a PUBLIC CHANNEL.
- One or more MALICIOUS ATTACKERS (called C or Charlie, E or Eve, O or Oscar).
- One or more MESSAGES.

Summary



Eve
Cryptanalysis
Alice
Bob
Encryption key
Decipherment key
Ciphertext
Plaintext
Encryption
Algorithm
Decryption
Algorithm
Plaintext

Agenda

- Introduction
- Basic Terminology
- The History of Cryptology
- Cryptology : Threats and Solutions :
  - Encryption
  - Hash
  - Electronic signature
- Basic Knowledge on Cryptanalysis
- Conclusion

The History of Cryptology

Four main periods:

- From 2000 years before J.C to 1000 after J.C => The first 3000 years;
- From 1000 to 1800 => the Awakening;
- From 1800 to 1970 => the rapid growth of the communications industry;
- From 1970 to the present time=> the « modern cryptology ».

The First 3000 Years (2000 BC to 1000 AD)

- Egypt
- Mesopotamia

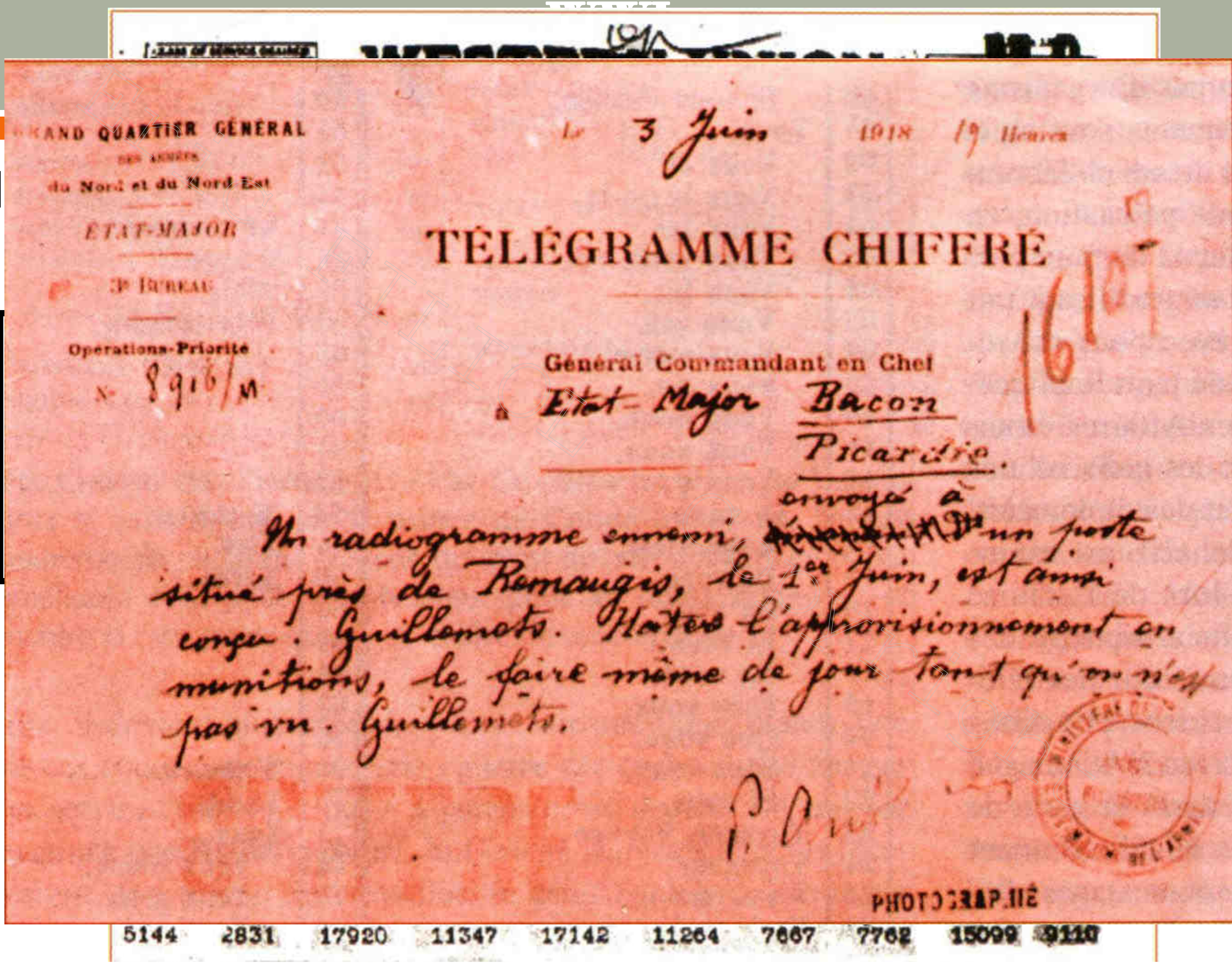
The Awakening Period (1000 AD to 1800 AD)

- The Middle Ages times :the loss of knowledge.
- The government cryptology was born in the 14th century. Appearance of “black chambers”.
- Around 1450, with the invention of printing, diplomats and militaries are using cipher more widely.
- The power of the “black chambers”decreased during the 18th century.

From1800 to 1970

- Communications and industry develop very quickly
- The inventions : the invention of the telegraph (1844), the railway, the radio (1895)...
- Strong need for information and communication protection
- The first steps of cryptology :
  - Kerckhoffs (1883) : military cryptography.
  - Kerckhoffs's principles applies nowadays to security.

M



GRAND QUARTIER GÉNÉRAL
DES ARMÉES
du Nord et du Nord Est
ÉTAT-MAJOR
3e BUREAU
Opérations-Priorité
N° 8916/M

Le 3 Juin 1918 19 Heures

TÉLÉGRAMME CHIFFRÉ

16107

Général Commandant en Chef
à Etat-Major Bacon
Picardie.

Un radiogramme ennemi, envoyé à ~~[illegible]~~ d'un poste situé près de Remaugis, le 1er Juin, est ainsi conçu. Guillemets. Hâtez l'approvisionnement en munitions, le faire même de jour tant qu'on n'est pas vu. Guillemets.

P. [illegible]

CHIFFRE

PHOTOGRAPHIÉ

5144 2831 17920 11347 17142 11264 7667 7762 15099 9110

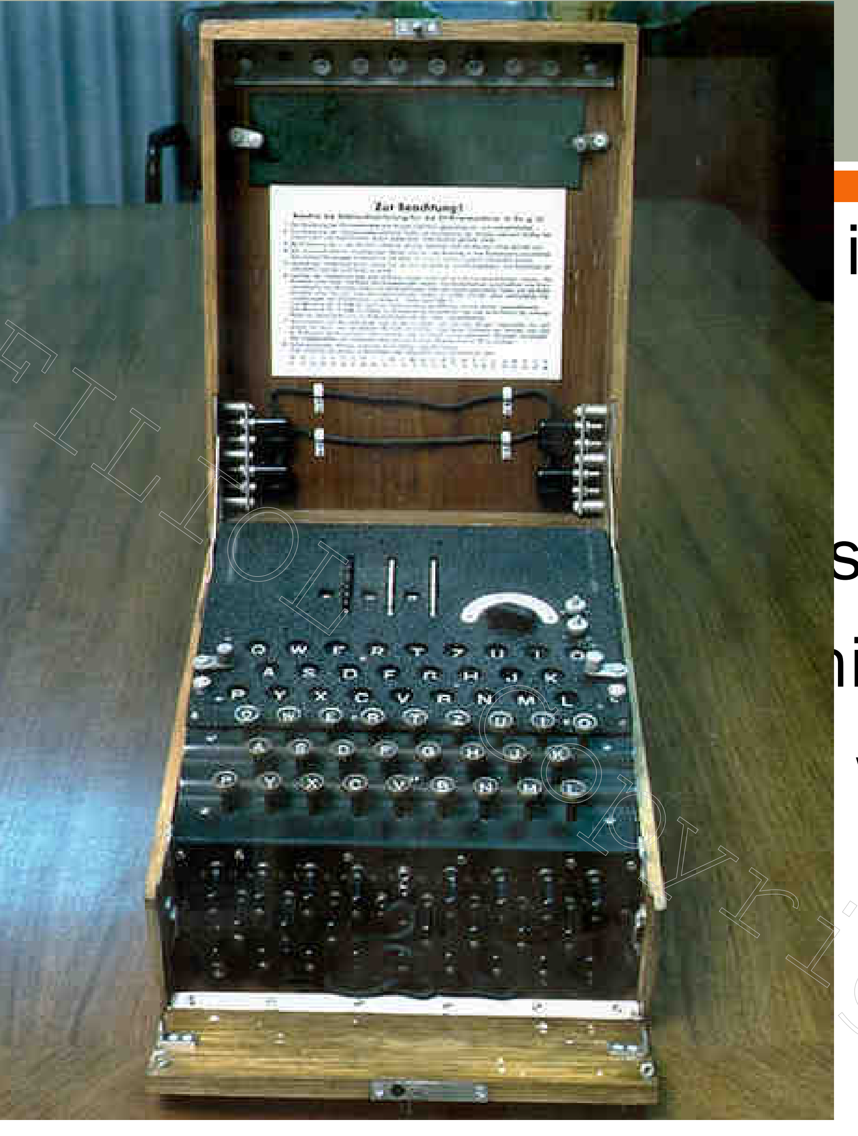
Betw

- Some countr importance of the cryptolog
  - Military er

➢ The first app s (1923).

➢ First analysis nigma.

➢ Red and Purp war.



WWII

- All the belligerents are competing for information.
- Secret projects of cryptanalysis (ULTRA, MAGIC).
- Cryptology plays a key role in the outcome of military battles (German invasion, Atlantic battle with U-boots, England battle, North Africa battle Pacific war, etc...).

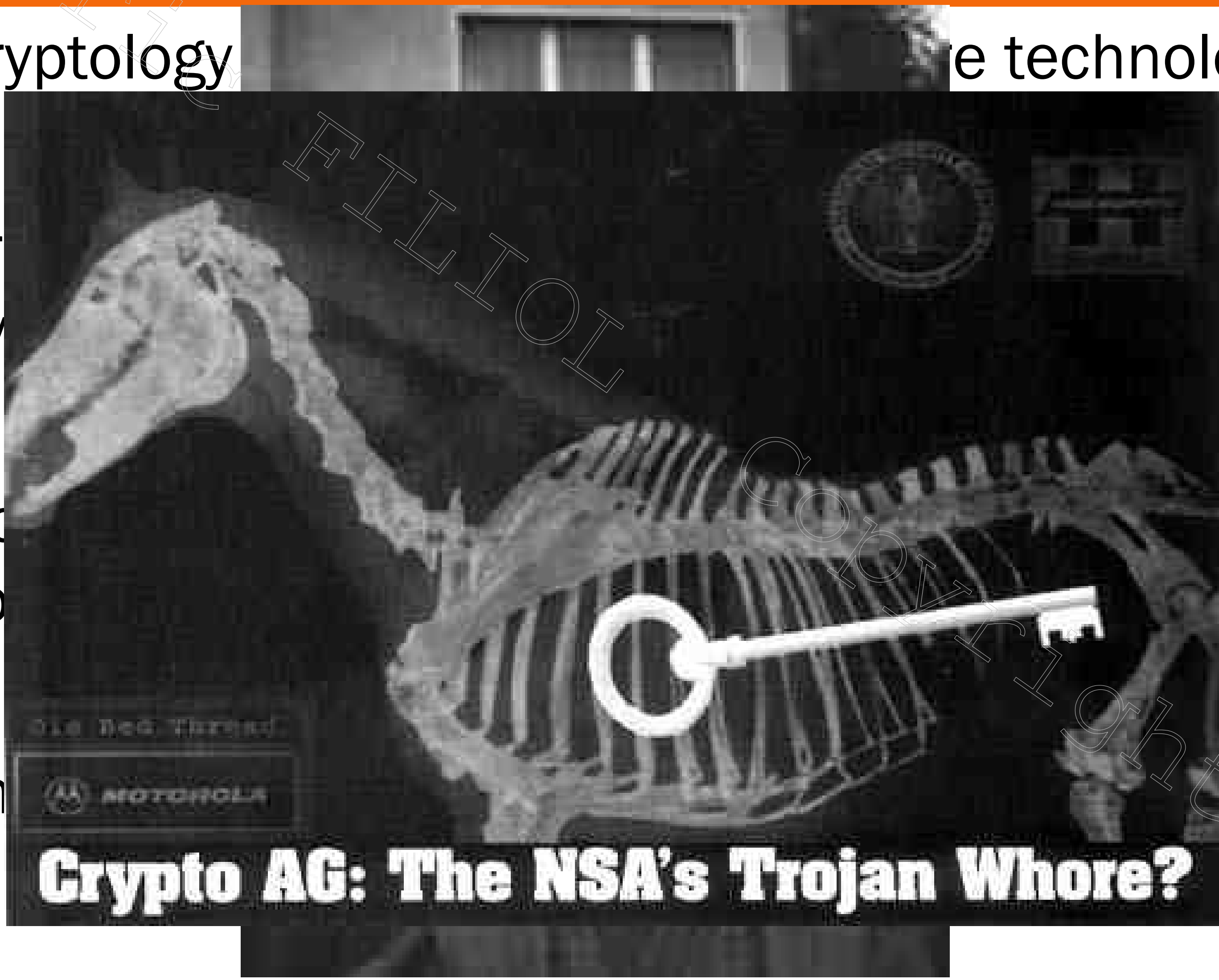
After World War II

- Cryptology e technology.

- Pr nications by

- Go d actual co

- Th nce.

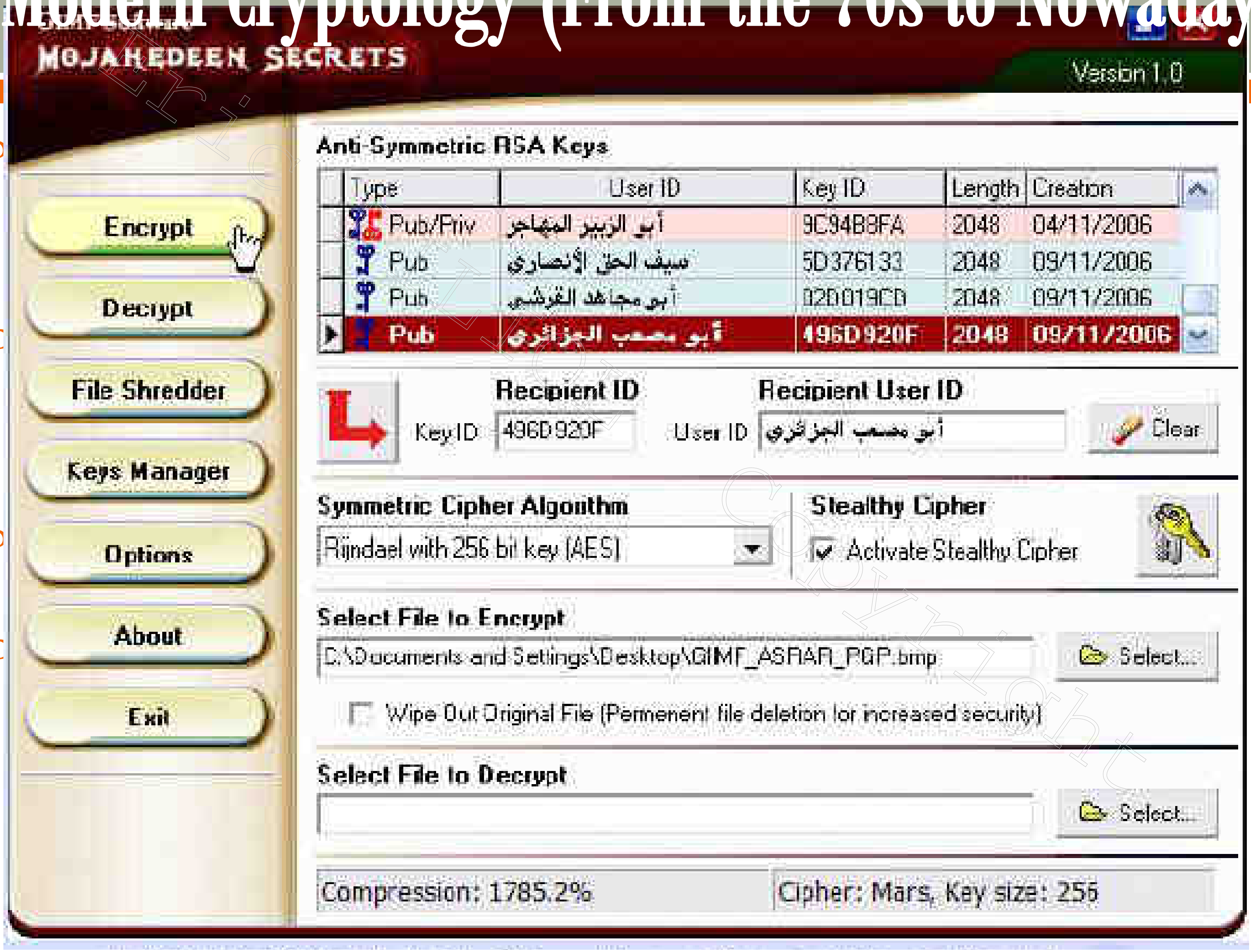


Modern Cryptology (From the 70s to Nowadays)

- Information society evolves to new needs.
- Birth of an actual civilian cryptology.
  - 1970 research carried out by Hans Feistel at IBM (Lucifer).
  - 1977 publication of the D.E.S (Data Encryption Standard).
  - 1977 Diffie et Hellman publish the following article :

    New Directions in Cryptography.
  - 1978 RSA system.

Modern Cryptology (From the 70s to Nowadays)



Agenda

- Introduction
- Basic Terminology
- The History of Cryptology
- Cryptology : Threats and Solutions :
  - Encryption
  - Hash
  - Electronic signature
- Basic Knowledge on Cryptanalysis
- Conclusion

Cryptographie is Everywhere…

- Credit cards, Pay television, mobile phones…
- Phone communications, public –key infrastructures à clefs, IFF traffic…
- Network protection, VoIP, cloud…
- Password, email,e-business, online payments…
- RFID, DRM…

Major Threats

- Eve listens to the message sent by Alice
  - Confidentiality issue.
- Eve sends a message to Bob spoofing Alice's identity.
  - Identification issue.
  - Authentification issue.
- Eve modifies a document or a message (content, metadata)
  - Integrity issue.
- Alice sends a message to Bob then denies it.
  - Signature issue.

Additional Threats

- Problem related to reception receipt and emission receipt (proof of emission and of reception).

- Forging the date of an email message, timestamp problem.

- TRANSEC (TRANSmission SECurity) Problems:
  - Communication jamming
  - Communication channel cut
  - Alice wants to hide that she sends a secret message (hiding the channel)

Solutions

Make sure of :

- Confidentiality :

  Data must remain non understandable to non-authorized persons

- Data integrity :

  The data cannot be modified nor created by an ennemy or by error (by a legitimate user)

- Authentification :

  Make sure of the identification (origin) and of the integrity (content) of the information ;

- Non deniability/signature :

  Mecanism which prevents from denying an action or a message.

Purposes/Tools

Provide information security using the following cryptographic techniques :

- **Encryption** (provides confidentiality)
- **Hashing** (provides integrity)
- Authentication
- **Digital signature** (provides authentication and non deniability)

Encrytion

- Cryptographic functionnality to enforce and provide data confidentiality.

- *<u>ENCRYPTION</u>: operation which consists to transform a plaintext into a ciphertext (cryptogram) by means of an algorithm and of one or more encryption keys.*
- *<u>DECRYPTION/DECIPHERMENT</u>: inverse operation which is performed with the same algorithm and one or more deciphering key(s).*

Encryption

There exist three types of encryption

1. Symmetric (or secret key) encryption (stream ciphers, block ciphers).

2. Asymmetric (or public key) encryption (RSA, EC)

3. Hybrid encryption systems (GPG, PGP)

Symmetric Encryption

- The emitter (Alice) and the recipient (Bob) share the same secret key.
  - Key management issue

- The encryption and the decryption keys are the same.
  - Keys are considered as random variables and hence any sequence of bits (of length the entropy of the key) is likely to be a valid key.

Stream Encryption

- **Stream cipher:** system which operate on each bit separately by using a transformation which depends on the time index defining the position of this bits in the sequence.

- The Vernam cryptosystem, which is also denoted one-time pad system, is the paradigm of stream ciphers.
  - o Encryption: M (ciphertext) ⊕ K (key) = C (ciphertext)
  - o Decryption: C ⊕ K = M

- From a practical point of view a random sequence is xored to the plaintext (encryption) or to the ciphertext (decryption)

Block Encryption

- **Block encryption:** encryption system which splits the plaintext (encryption) or the ciphertext (decryption) into fixed-size chunks of bits and which encrypt each block separately with the same key. Block size are generally of 64 (DES, Blowfish) or 128 bits (AES).
- Two main families of block ciphers:
  - Feistel schemes (H. Feistel, 1975) like DES or MARS
  - Substitution/permutation networks like AES

Symmetric Encryption

- Pros:
  - Highest encryption speed (bitwise xor)
  - Can realize perfect secrecy (illustration)

- Cons:
  - Key management issues.
  - Perfect secrecy is difficult to manage (perfect random sequence that must be as long as the message).

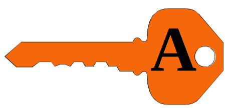
Asymmetric Encryption

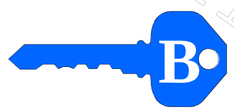
- Alice & Bob have a private key (secret) each and a public key each
- Public keys are published in a public directory and can be accessed by anyone.

Alice

Bob

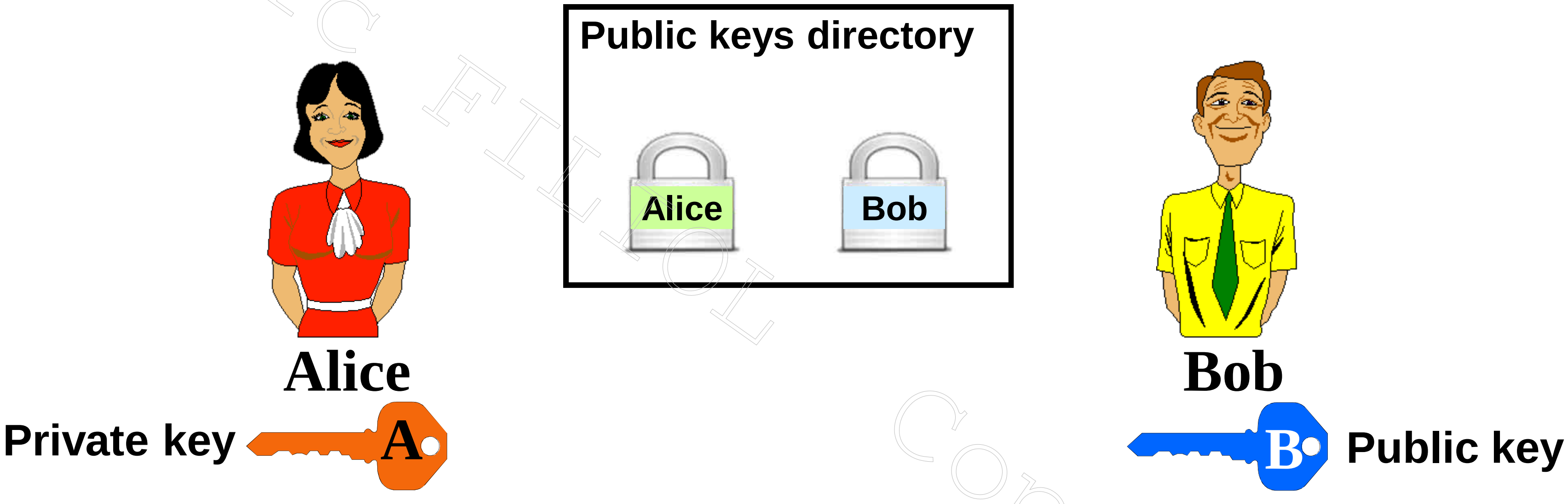
Private key



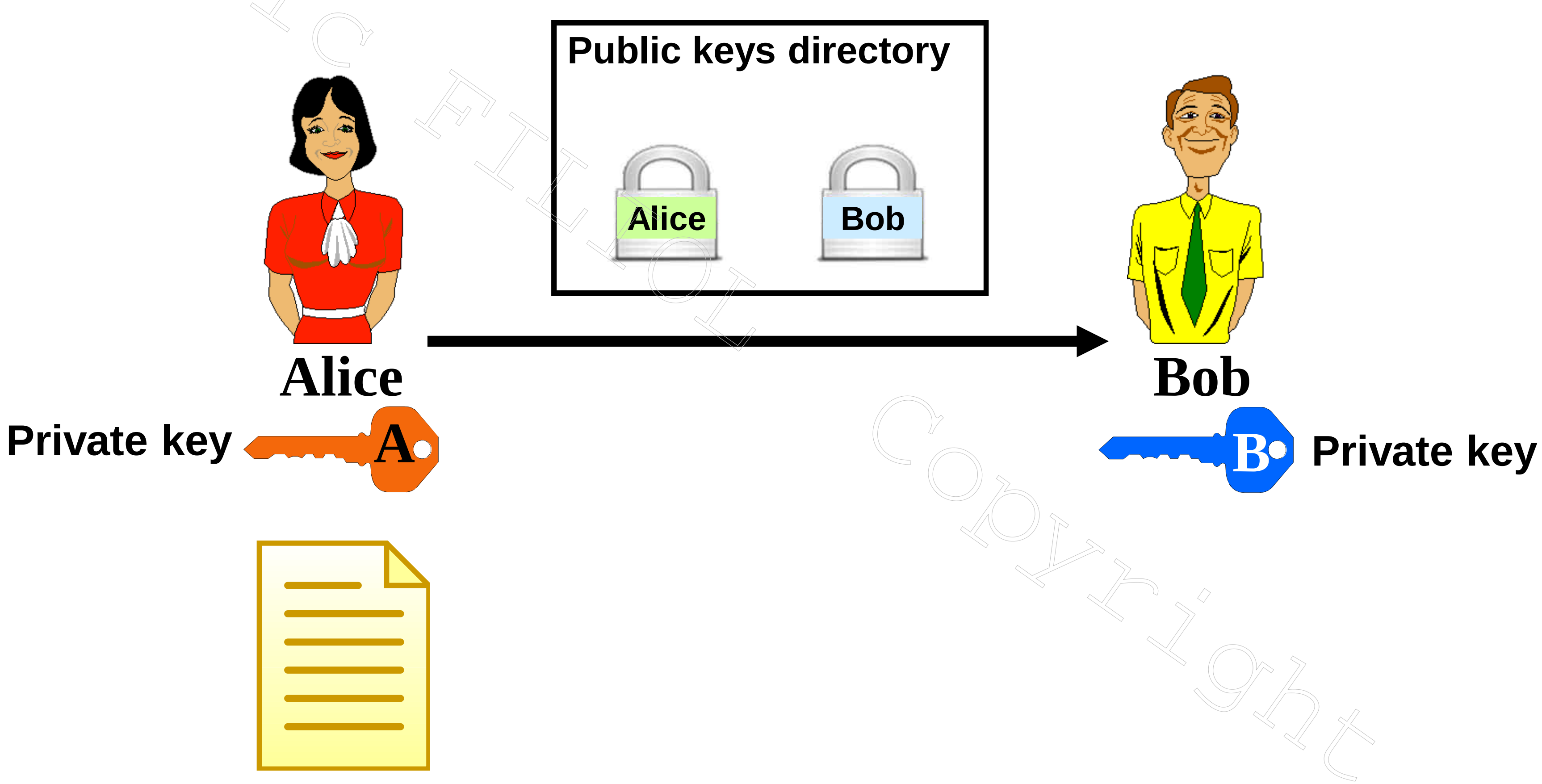


Private key

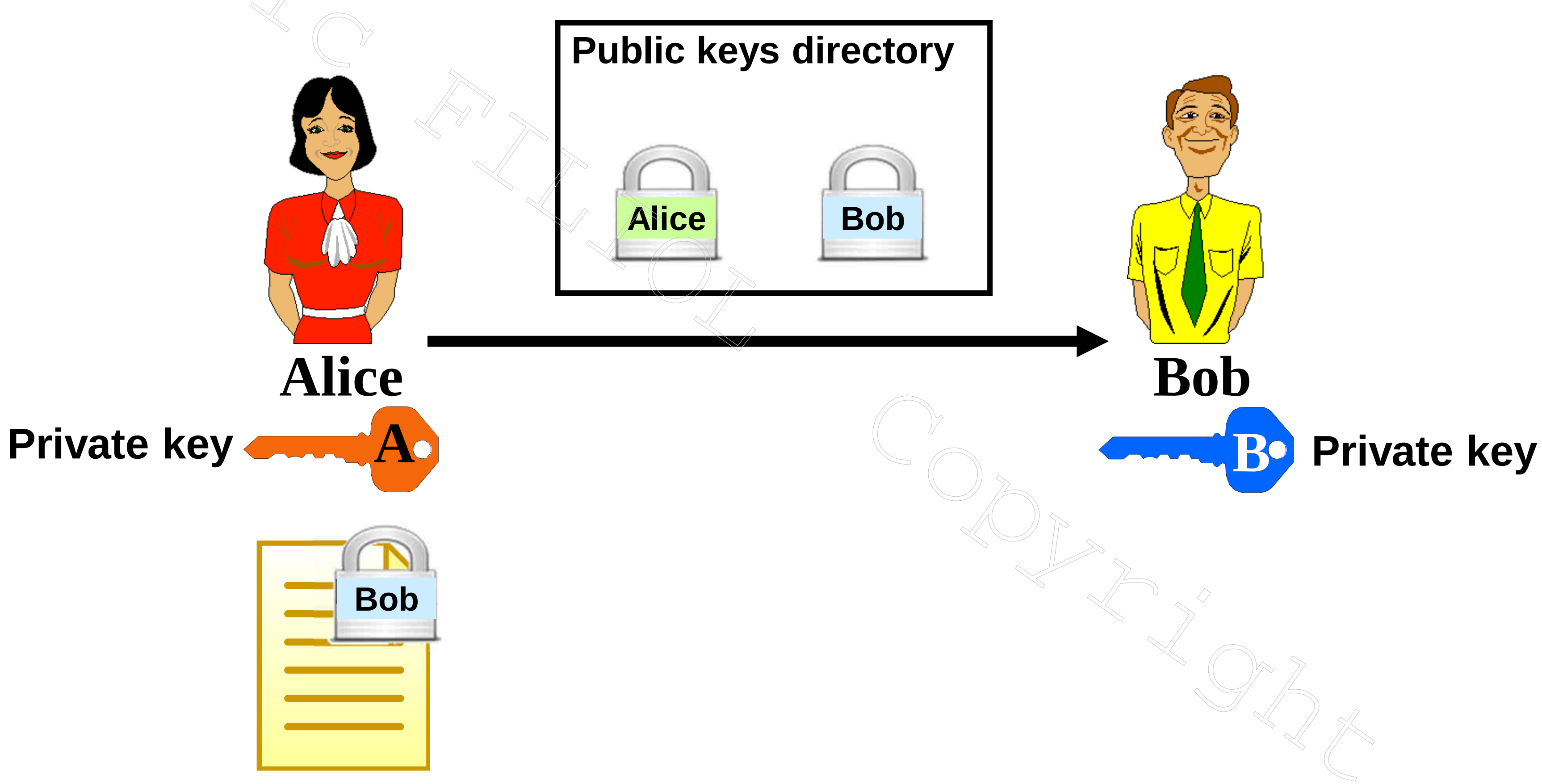
Asymmetric Encryption



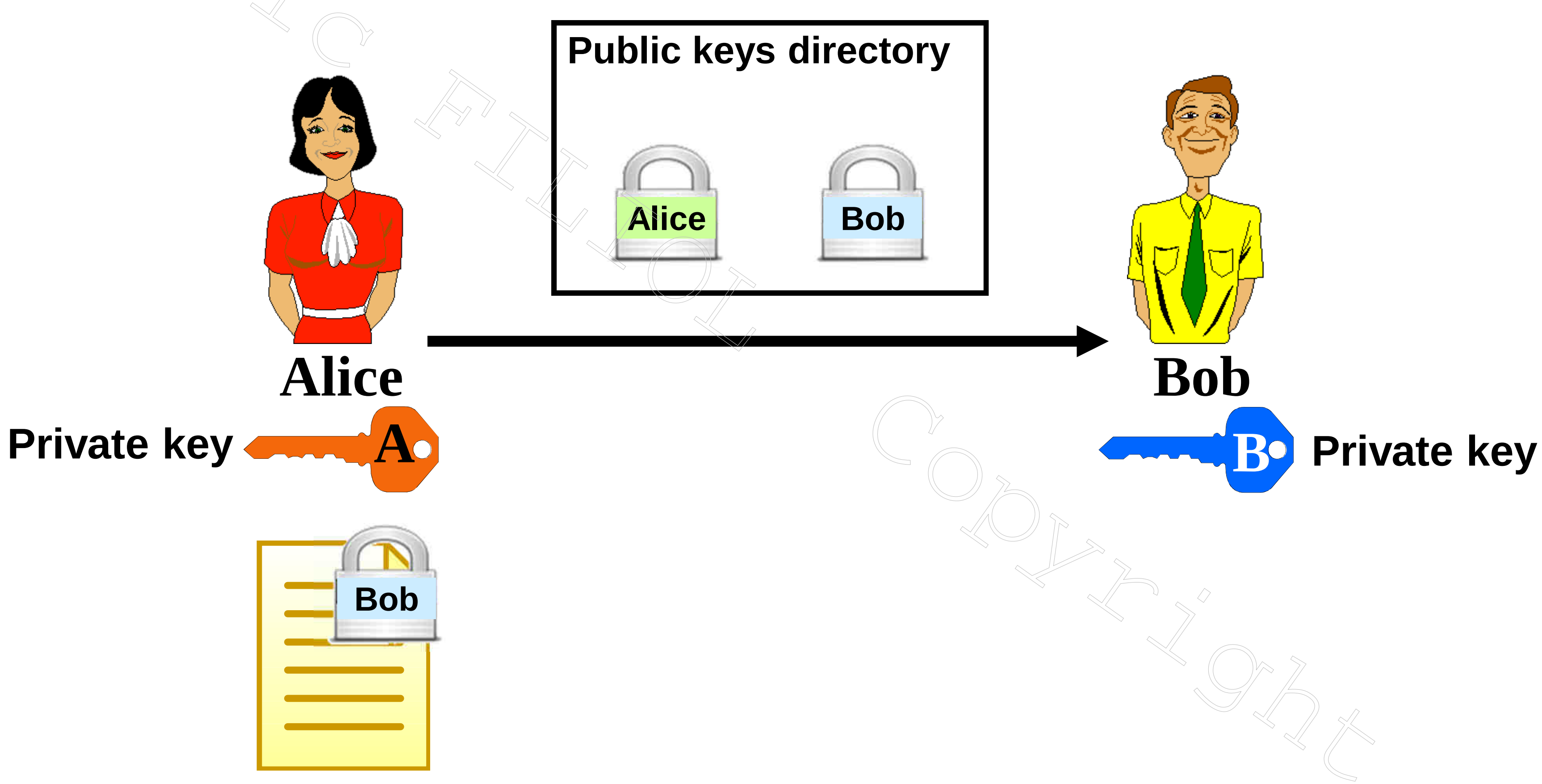
Asymmetric Encryption



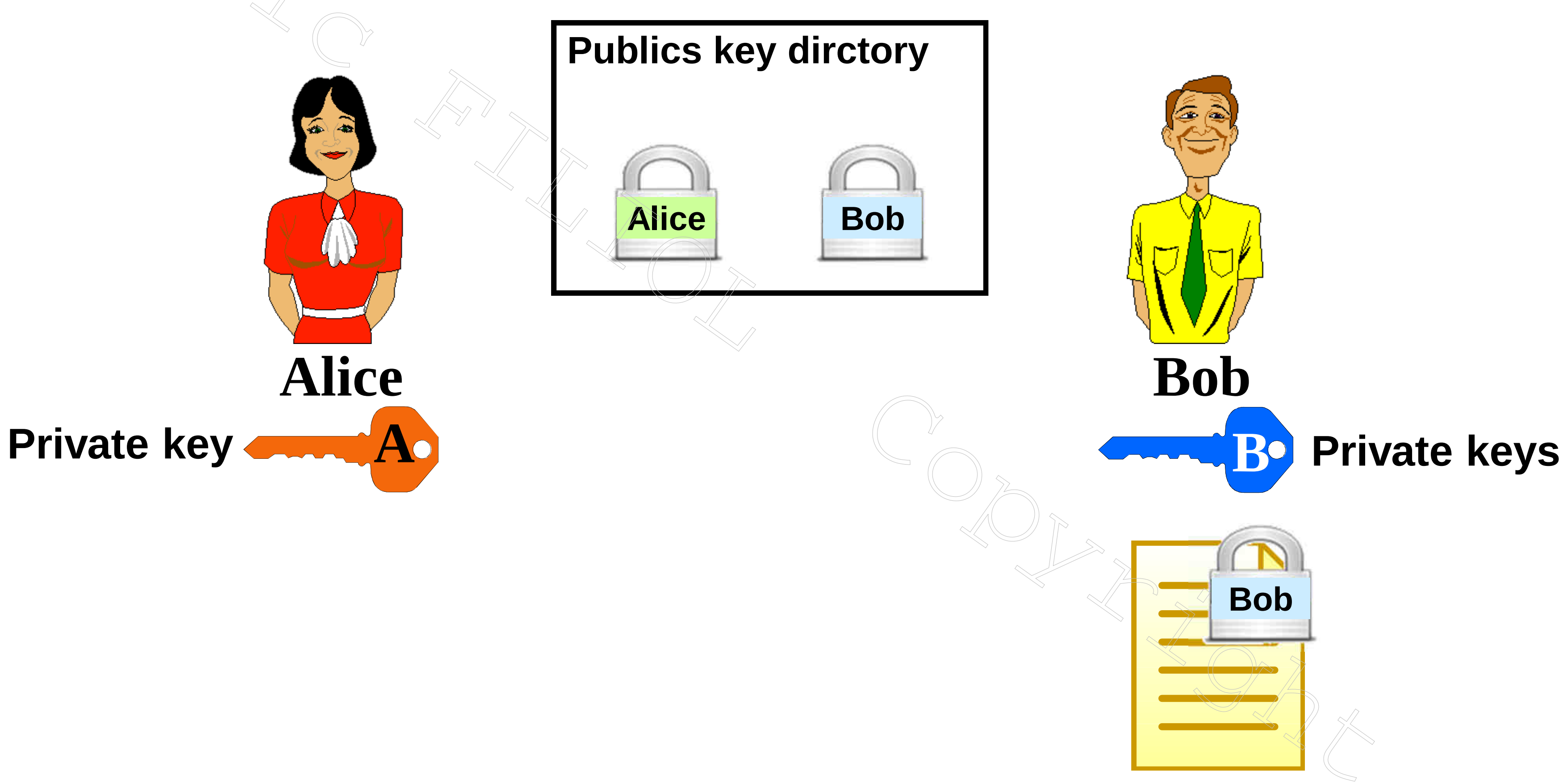
Asymmetric Encryption



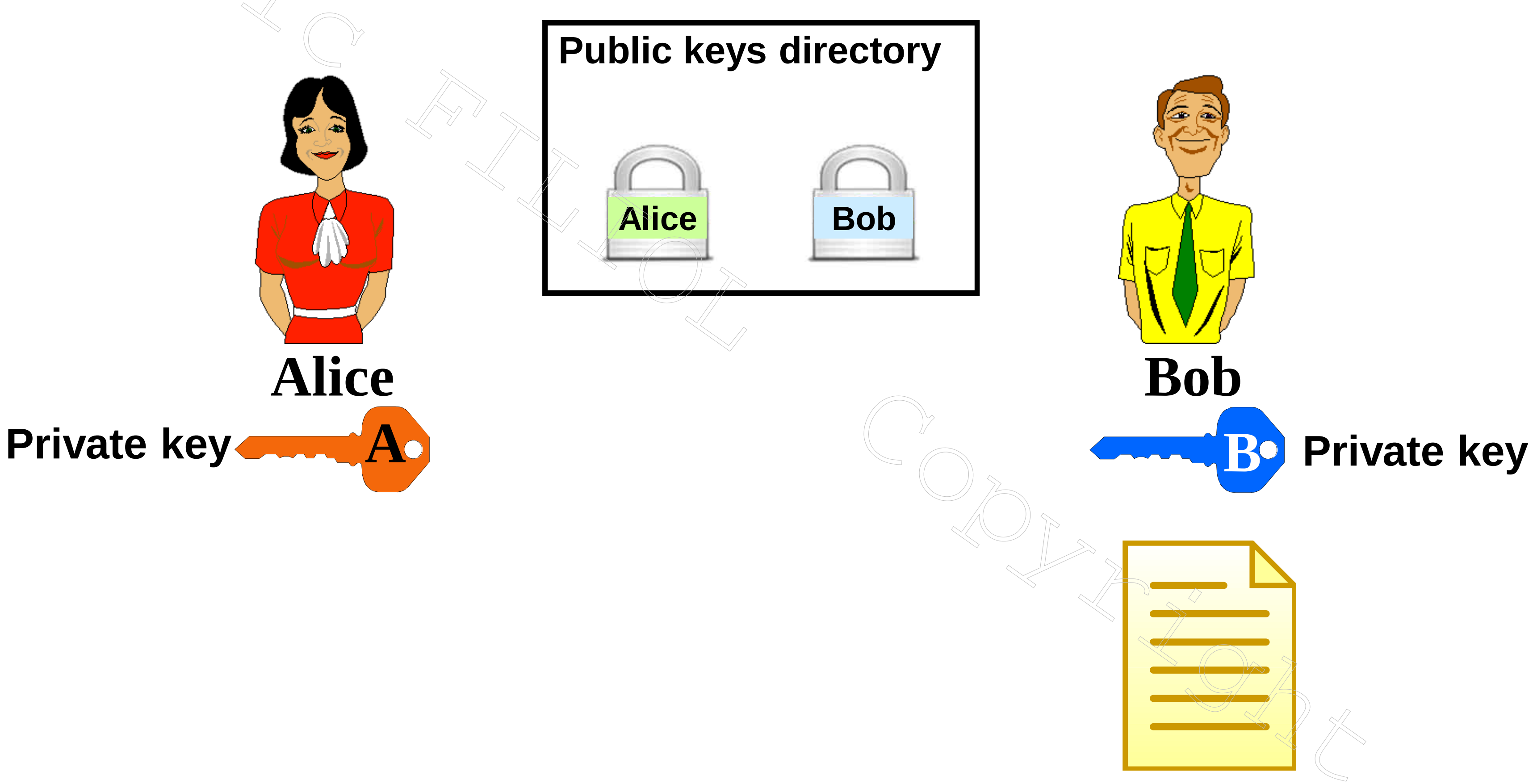
Asymmetric Encryption



Asymmetric Encryption



Asymmetric Encryption



Asymmetric Encryption

- Alice & Bob have each a pair of {public, private} keys. Public are accessible to anyone.

- Alice encrypts a message using Bob's private key and sends the message to him.

- Bob deciphers the message using his private key.

- Encryption is then performed using the recipient's private key while decipherment is performed using the related private key.

A bit of maths... ??§∞∫!*

- All asymmetric systems use **one-way function with trapdoors.**

- One-way functions (OWF)

  A function f : M -> C is an OWF if and only if:

  - It is computationally easy to compute f(m) from m,
  - It is computationally intractable to compute m from f(m),

- An OWF f is said to have a trapdoor or to be trapdoored if with f(m) and an additional information (in RSA the private key) we can compute m easily.

A bit of maths... ??§∞∫!*

- Most asymmetric systems lies on computationally intractable problems: factoring, quadratic residues, discrete logarithm, sphere packing...

- The security of those systems lies on the assumption that there would exist actual computationally intractable problems.

- This assumption has never been mathematically proved (P = NP or not conjecture).

Asymmetric Encryption

- Pros
  - No prior key exchange required
- Cons
  - Very low encryption speed
  - No proof of security. Just an assumption!

Symmetric vs asymmetric encryption

	Symmetic Systems	Asymmetric Systems
Existence	For centuries	Less than 40 years
Security	Theoretically and practically secures	Lies on complexity assumption (security is assumed but not proved)
Encryption speed	Very high	slow
Key	Secret key	(private key, public key)
Key management	Prior key sharing	PKI

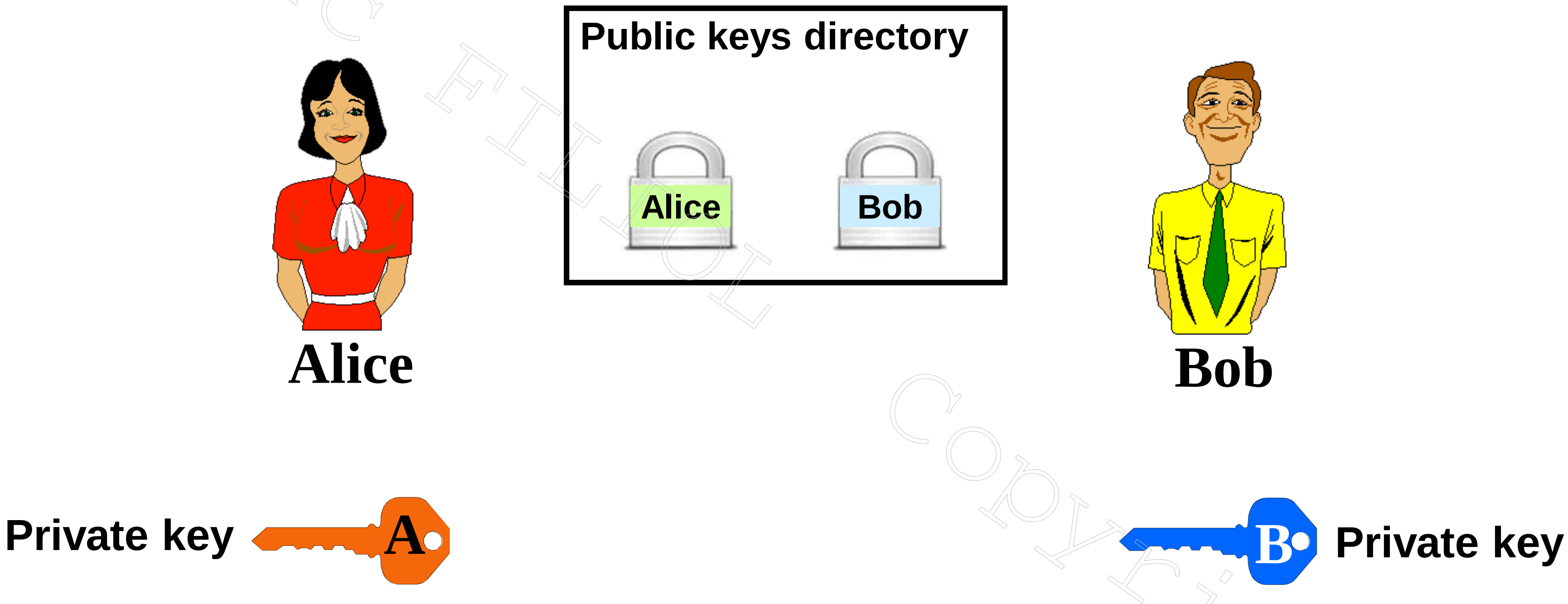
Hybrid Encryption

- It combine the key features of both worlds thus making asymmetric encryption usable in practice.

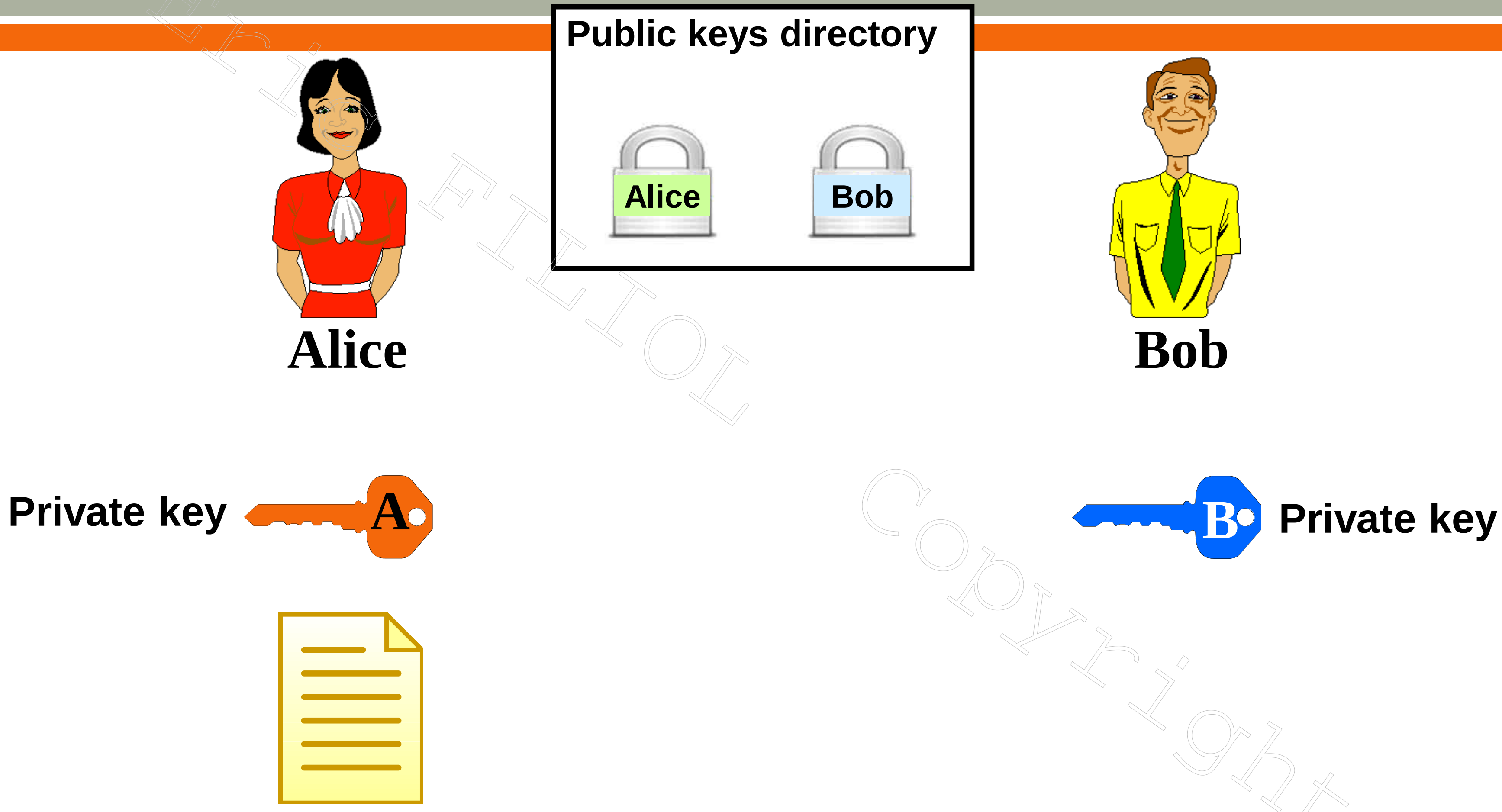
- Principle:
  - The message en encrypted by symmetric encryption.
  - The message key used is encrypted by asymmetric encryption.
  - Both encrypted message and encrypted message key are sent.

- Known systems
  - PGP
  - GPG

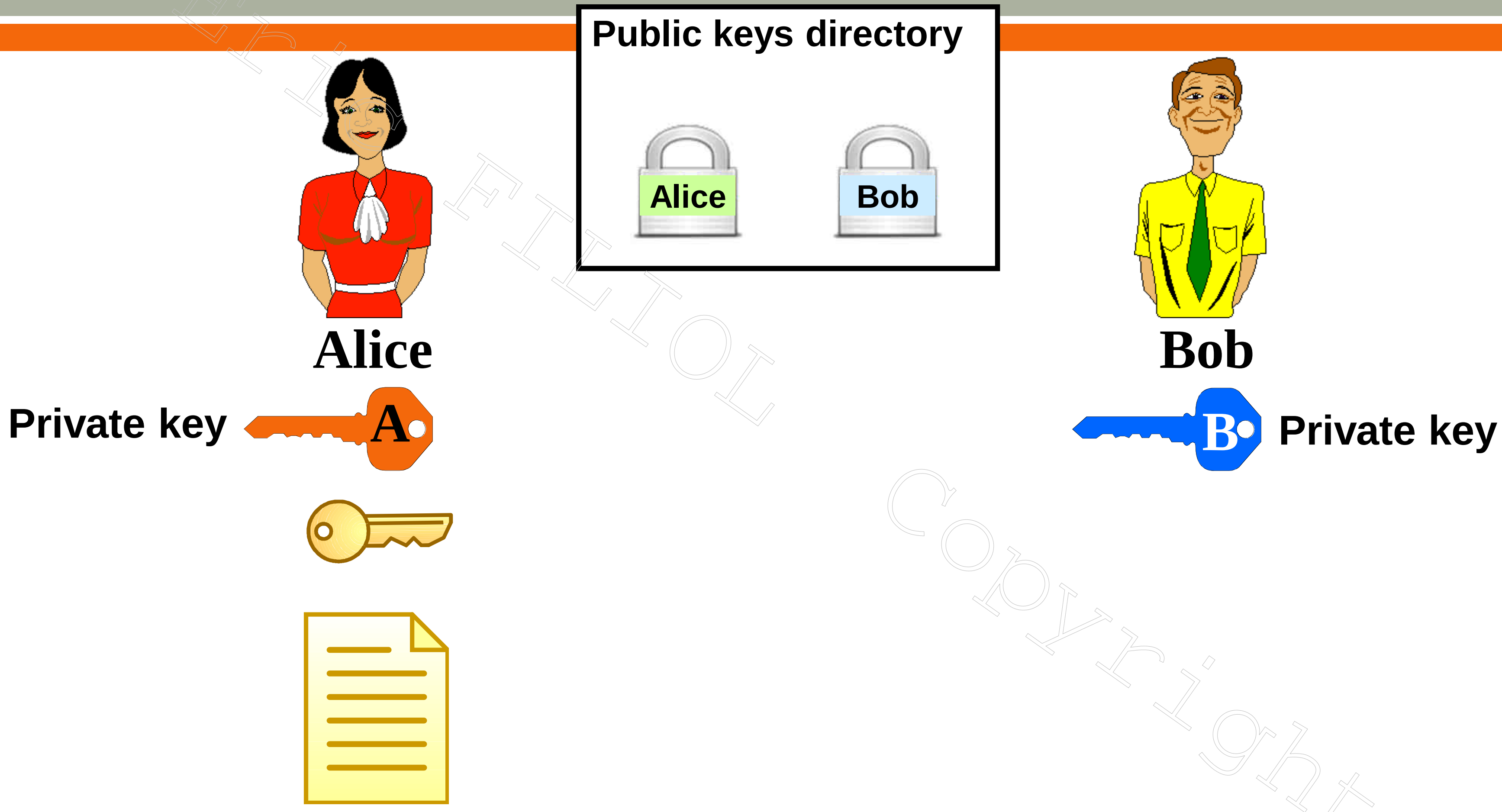
Hybrid Encryption



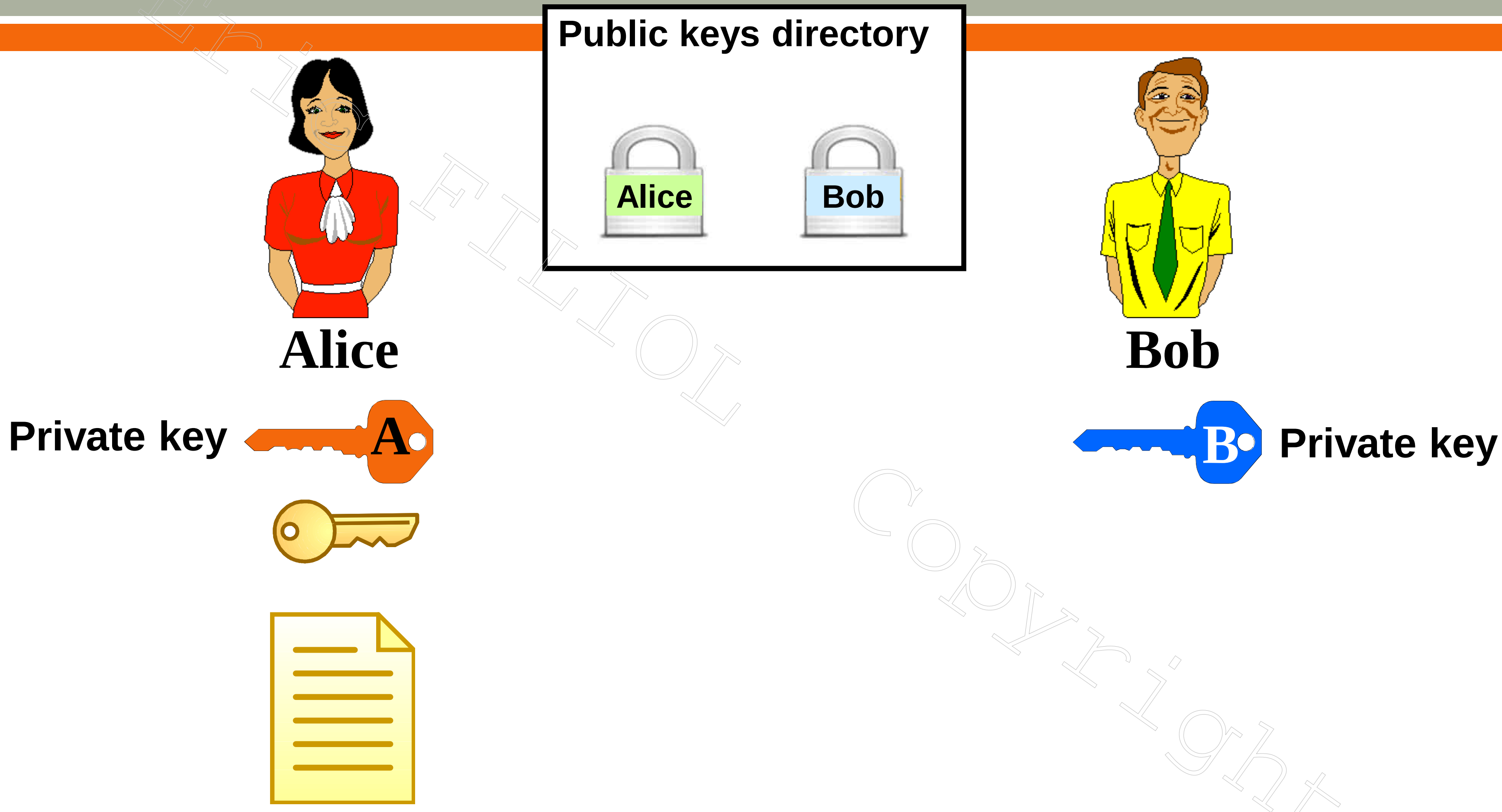
Hybrid Encryption



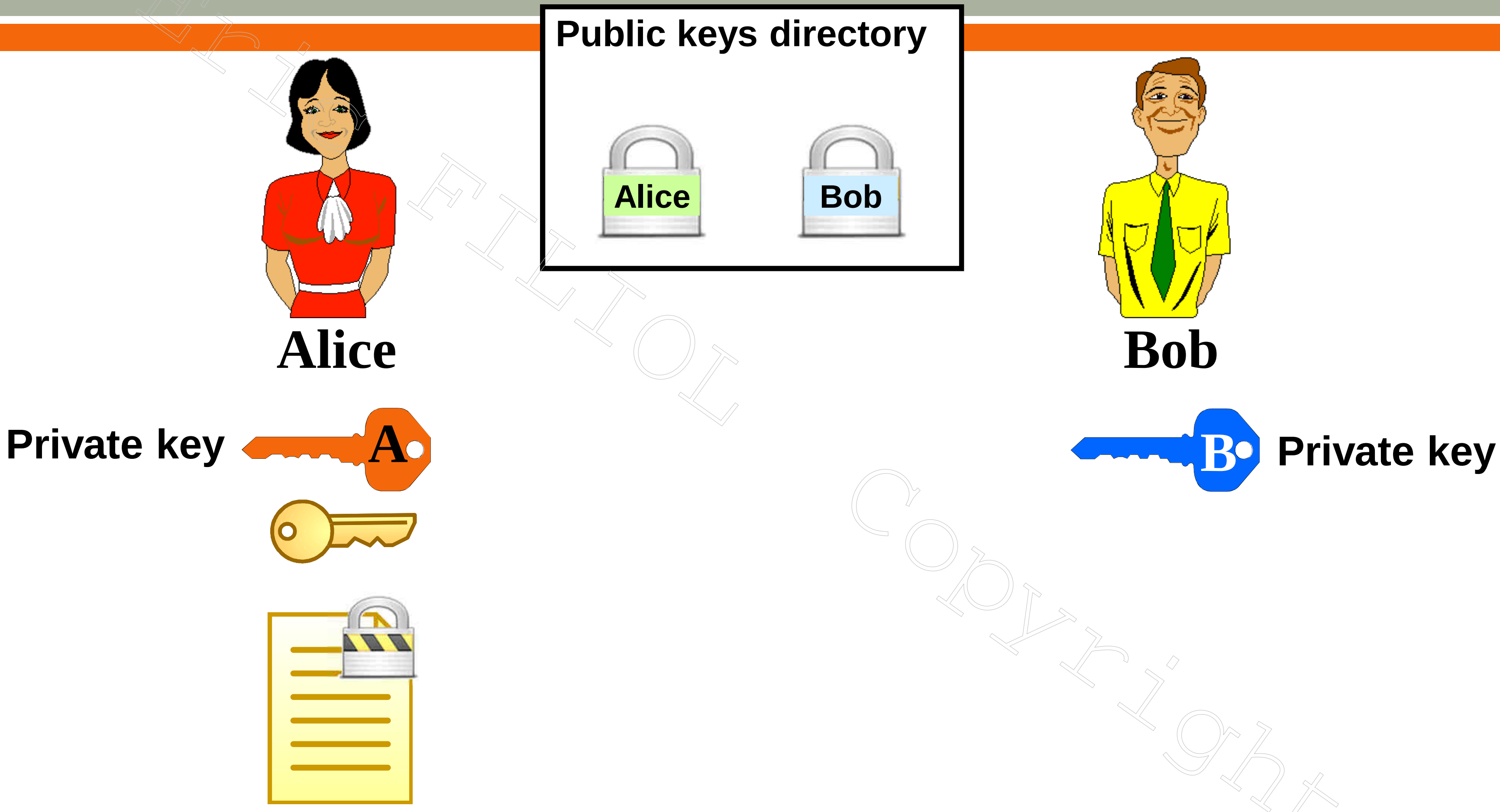
Hybrid Encryption



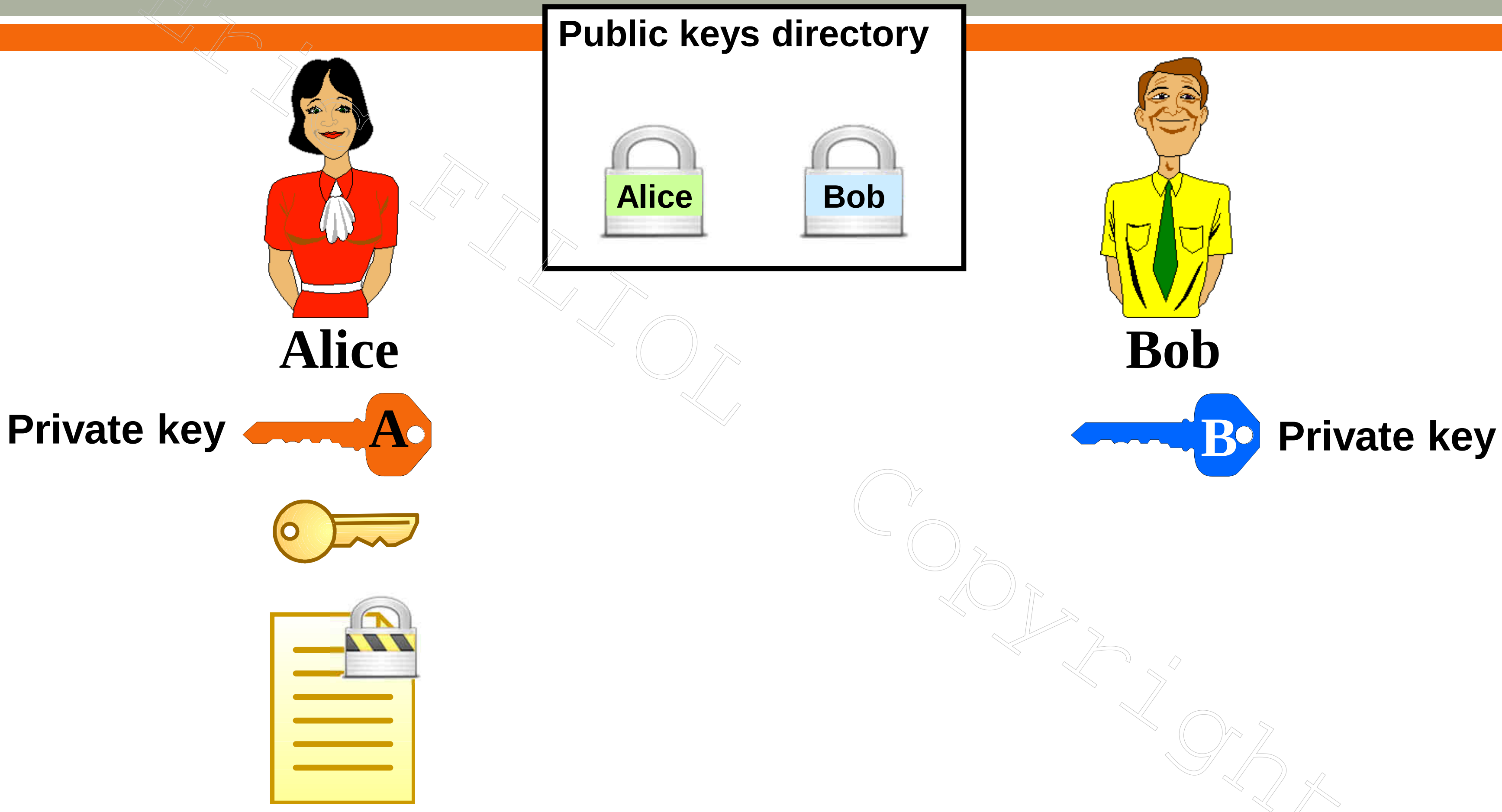
Hybrid Encryption



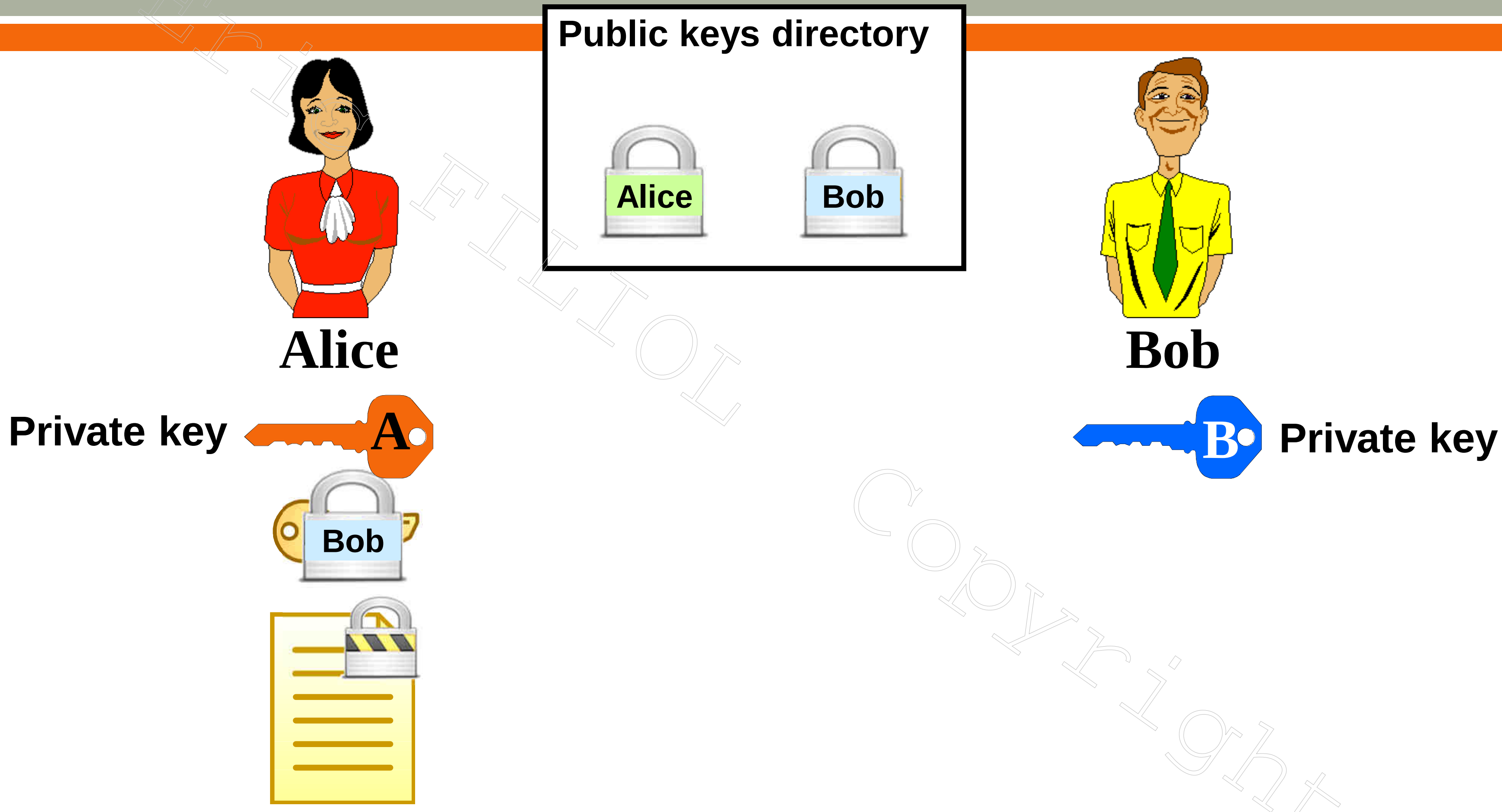
Hybrid Encryption



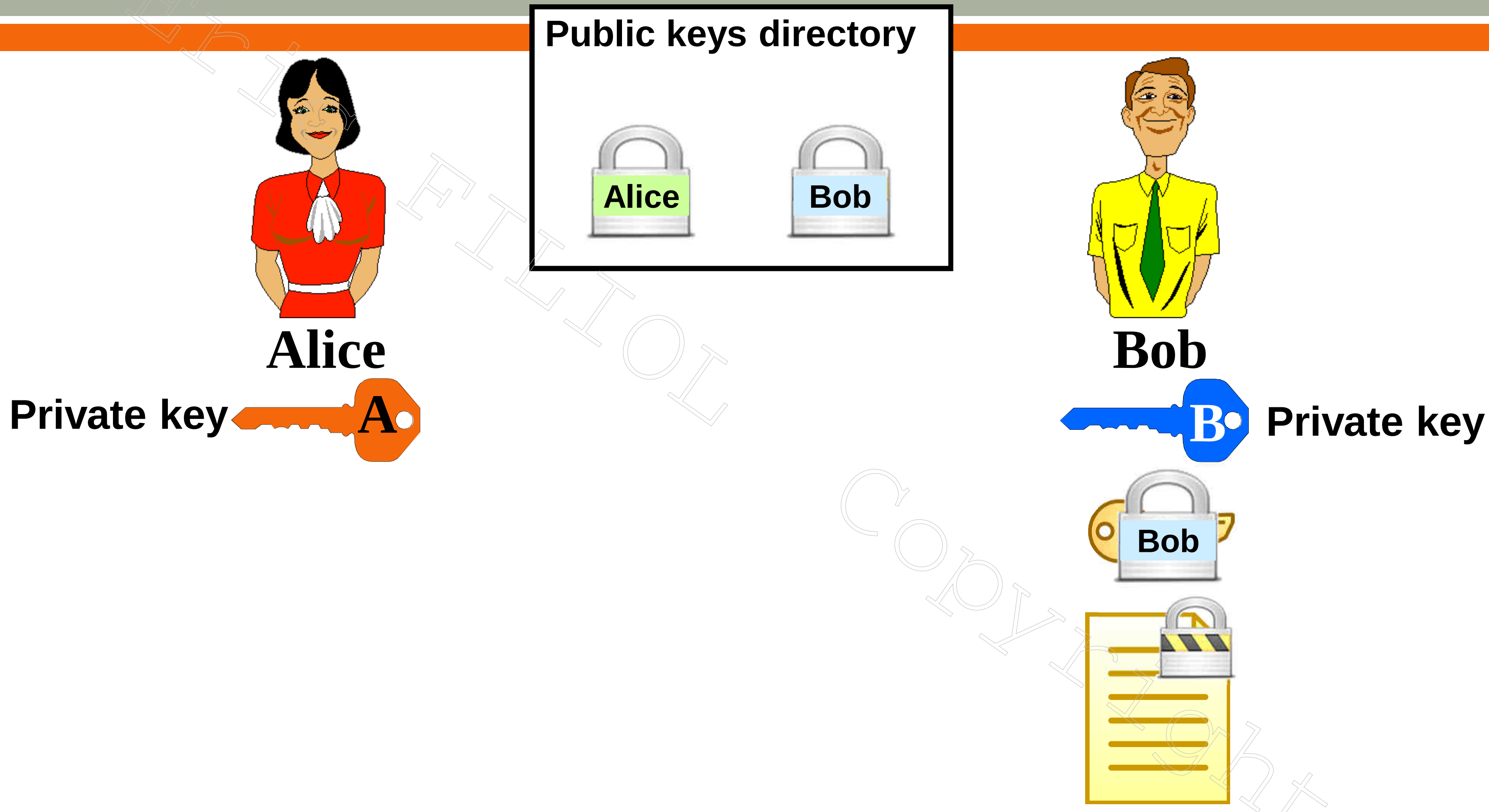
Hybrid Encryption



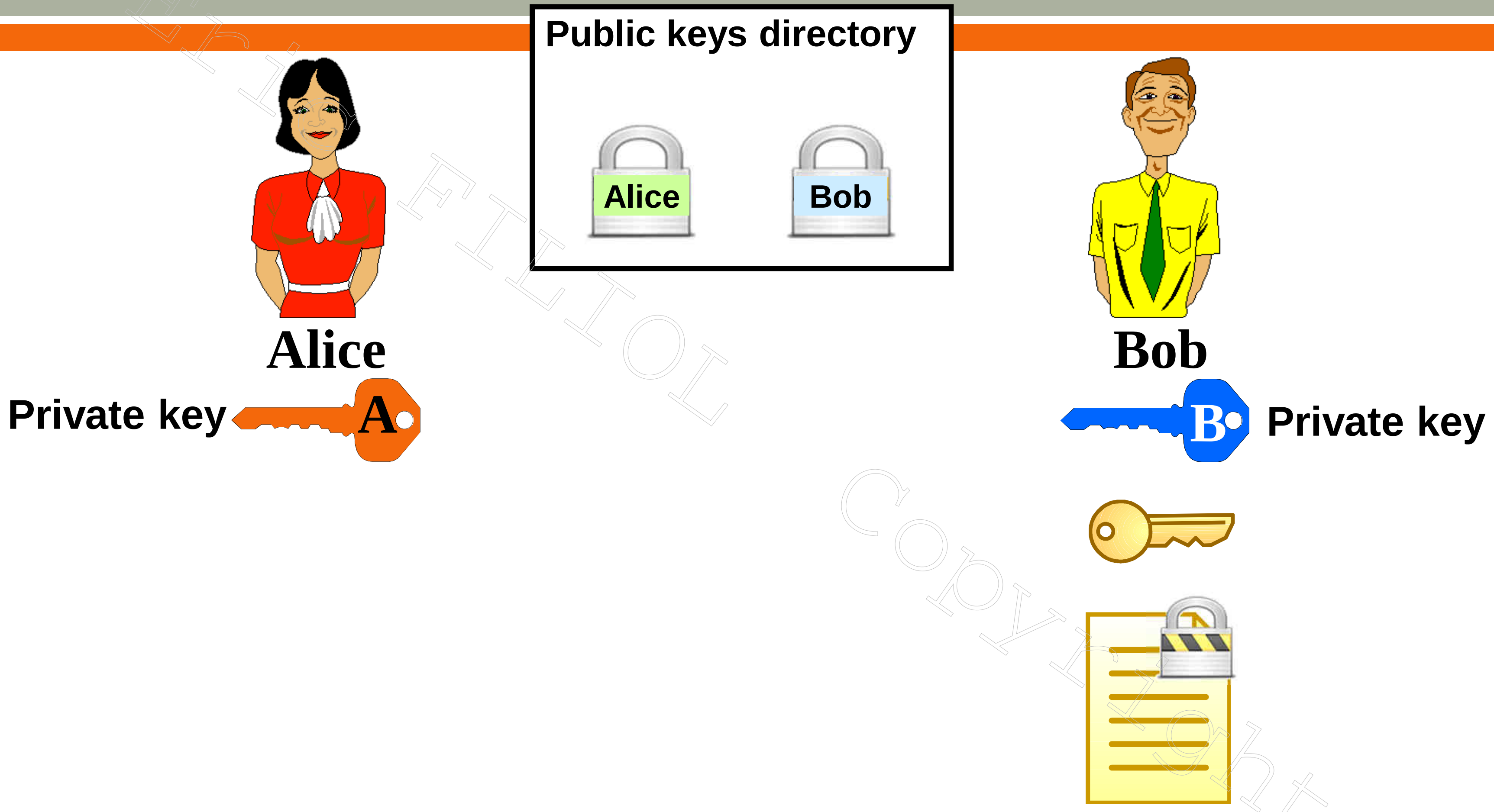
Hybrid Encryption



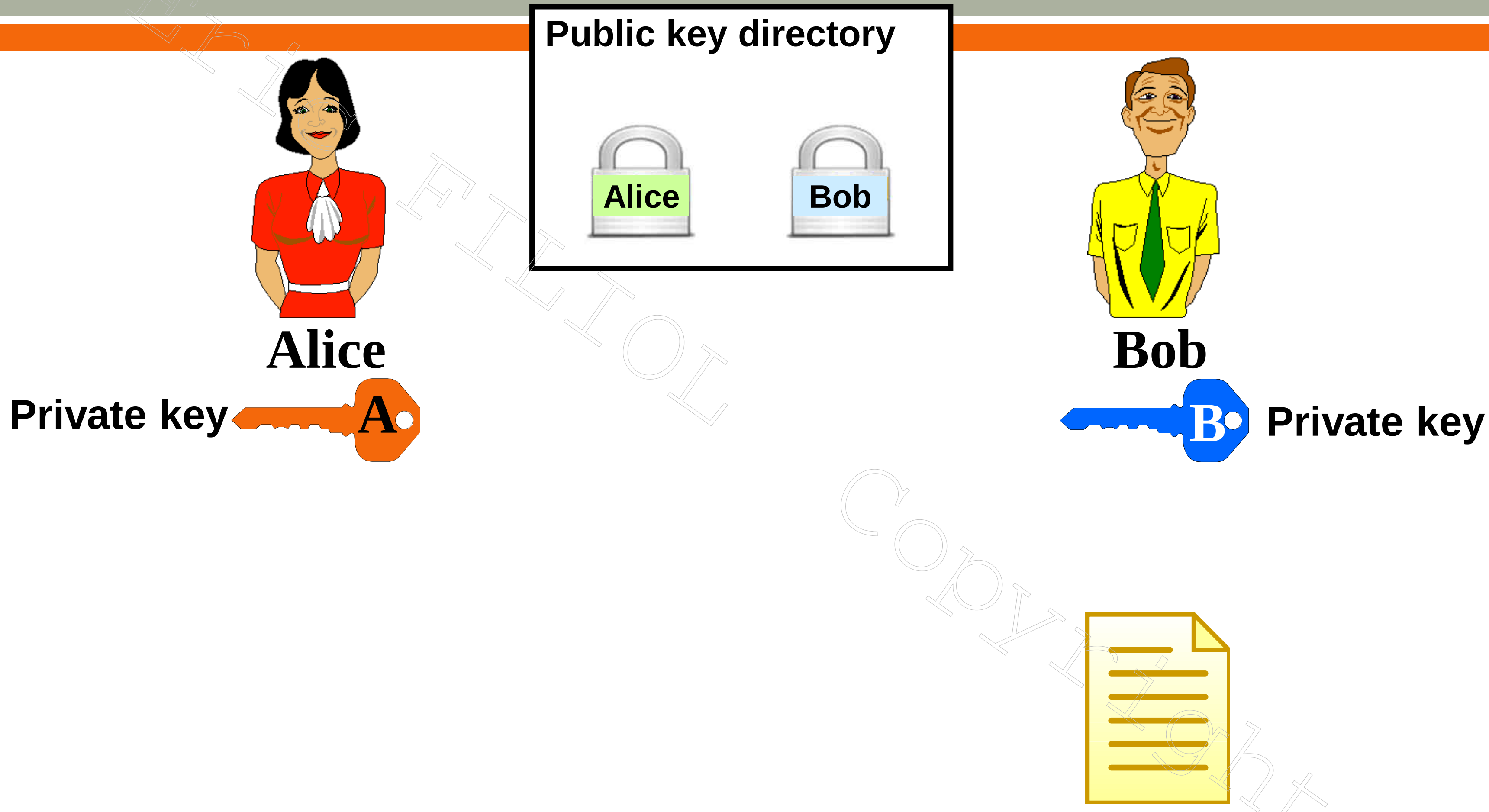
Hybrid Encryption



Hybrid Encryption



Hybrid Encryption



Hybrid Encryption

- Alice encrypts her message :
  - The system randomly generates a symmetric key K_{sym}
  - The message is encryptd with K_{sym}
  - K_{sym} is encrypted with Bob's public key.

- Bob deciphers the message :
  - Bob deciphers the key K_{sym} using his private key
  - Then he deciphers the message using K_{sym}

Agenda

- Introduction
- Basic Terminology
- The History of Cryptology
- Cryptology : Threats and Solutions :
  - Encryption
  - Hash
  - Electronic signature
- Basic Knowledge on Cryptanalysis
- Conclusion

Integrity & Hashing

- **Hash function:** transformation of a message of any size into a fixed-size (128, 160, 256, 512 bits) called hashed value.
  - Exemples: MD5, SHA-1, RIPEMD-160, SHA-256, SHA-512, Whirlpool.
- H is a hash function if and only if:
  - H(M) can be computed easily from M.
  - H collision-free: from M and H(M) it is computationally intractable to find M'≠M such that H(M') = H(M).

- Mathematical analysis

Integrity & Hashing

- Hashing provides integrity

  Message Integrity Code (MIC)

- Authentification is provided with an additional secret

  Message Authentication Code (MAC)

Agenda

- Introduction
- Basic Terminology
- The History of Cryptology
- Cryptology : Threats and Solutions :
  - Encryption
  - Hash
  - Electronic signature
- Basic Knowledge on Cryptanalysis
- Conclusion

Authentication

- Alice sends a message to Bob.
- We say that Bob identifies Alice if and only if
    1. Alice can prove to Bob that she is indeed Alice.
    2. Any other person **Eve** $\neq$ **Alice** cannot do the same (ie spoof **Alice**'s identity)
- We must also authenticate the messages that are sent.
    - Messages' integrity must be taken into account.

AUTHENTICATION = IDENTIFICATION + INTEGRITY

- In this respect biometry does not provide actual authentication
    - iPhone 5 recent case

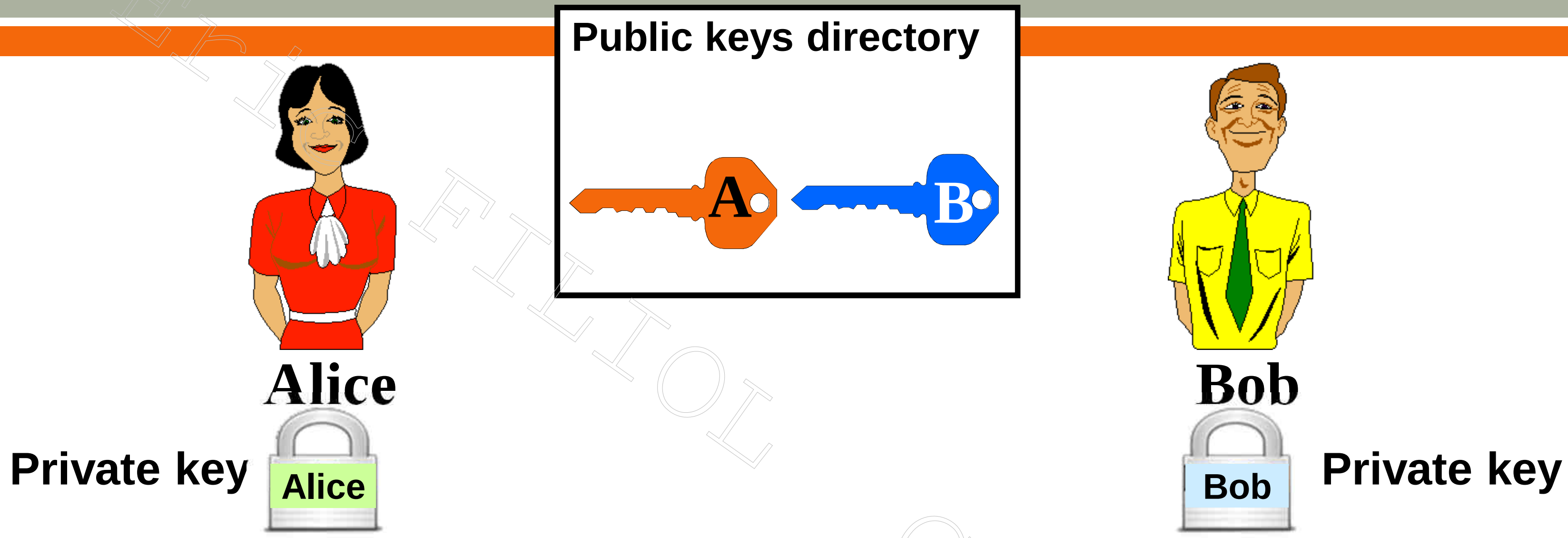
Digital Signature

- A message M is digitally signed by Alice if and only if:
  1. Alice can prove to Bob that she is indeed Alice.
  2. Any other person Eve ≠ Alice cannot do the same (ie spoof Alice's identity)
  3. Bob can prove to a third party D that only Alice can be the message author.

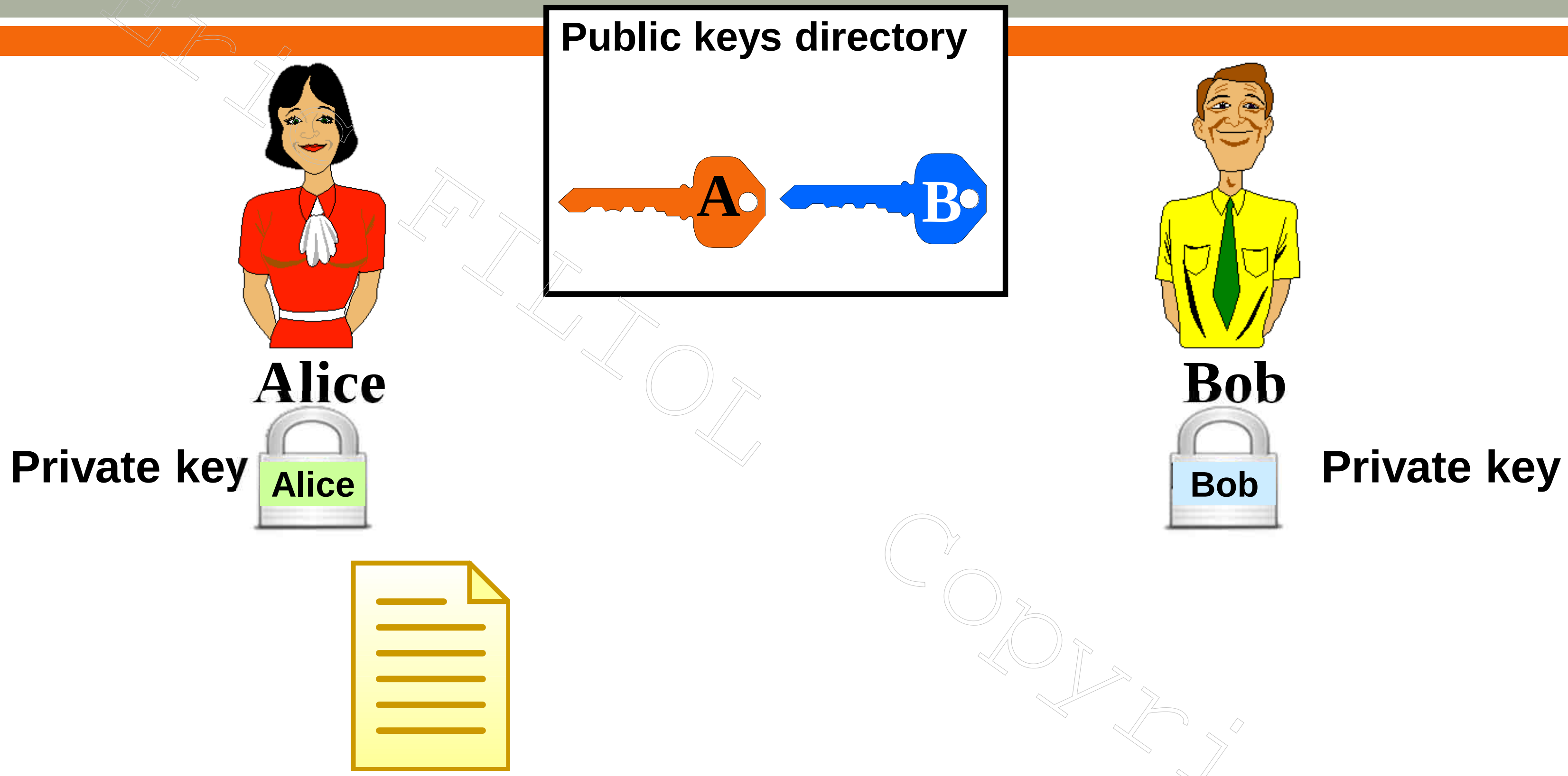
- If D = Alice then NON REPUDIATION/NON DENIABILITY by Alice.

SIGNATURE = AUTHENTIFICATION + CONVICTION TRANSFERT

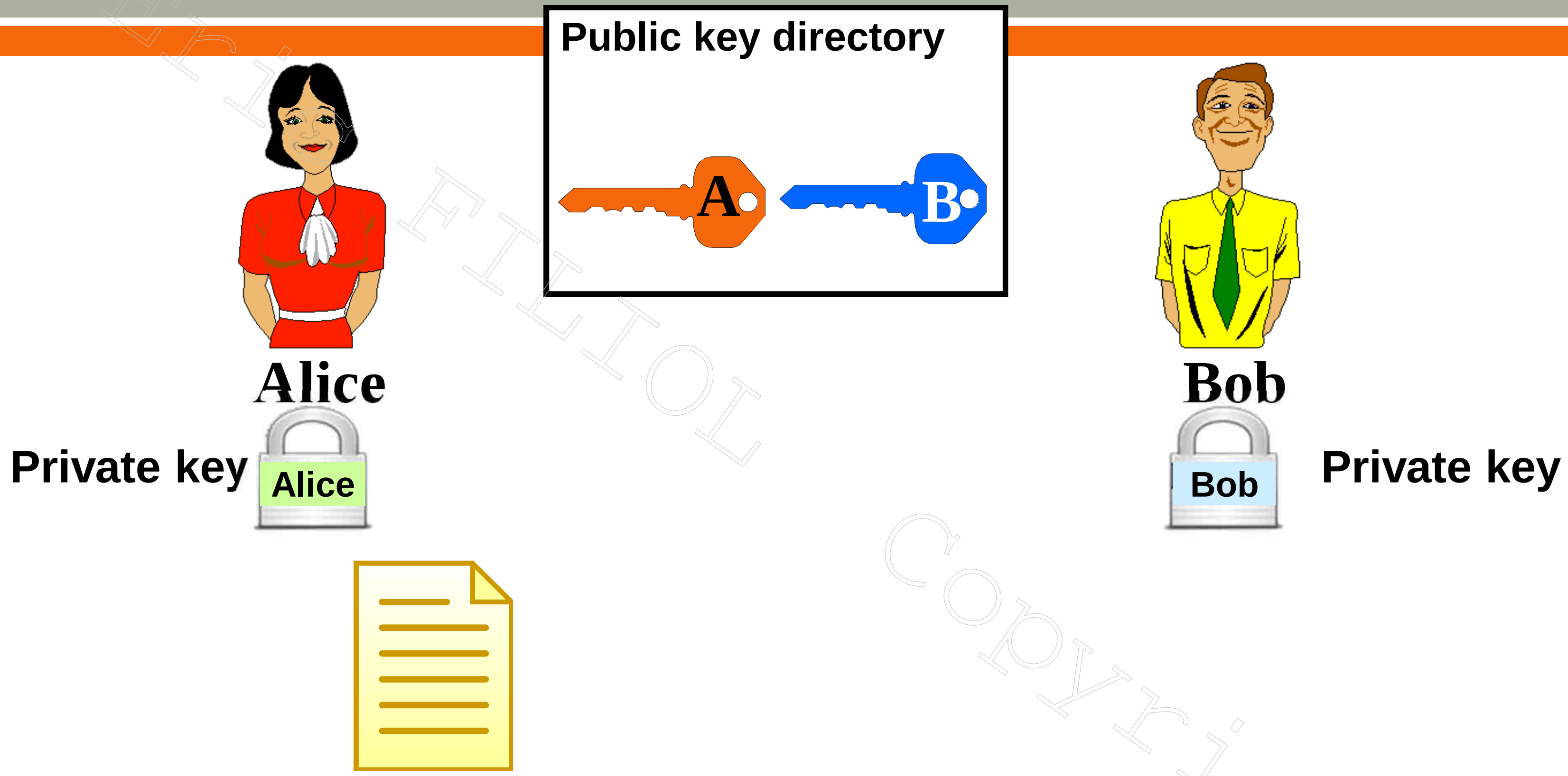
Digital Signature



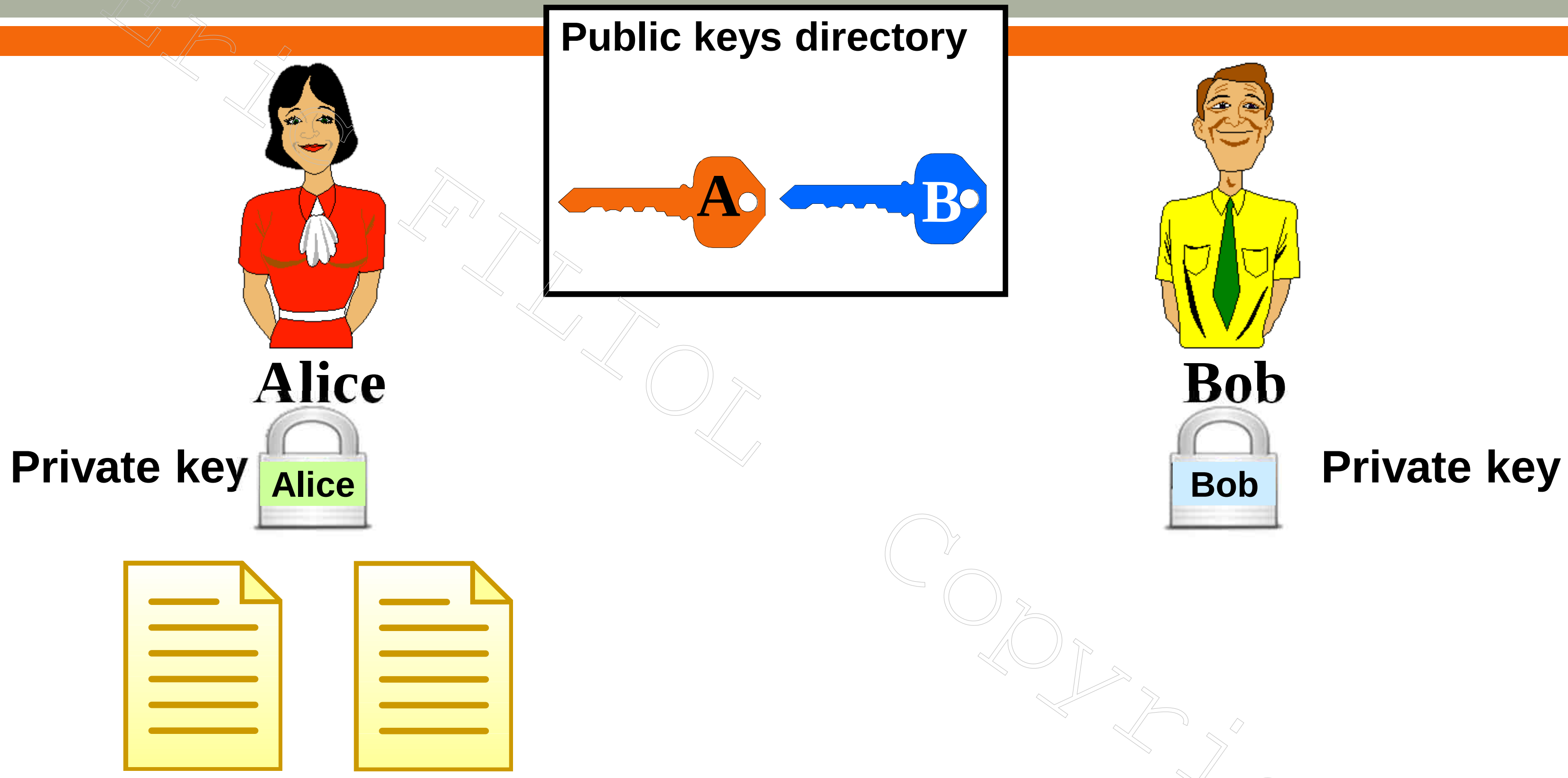
Digital Signature



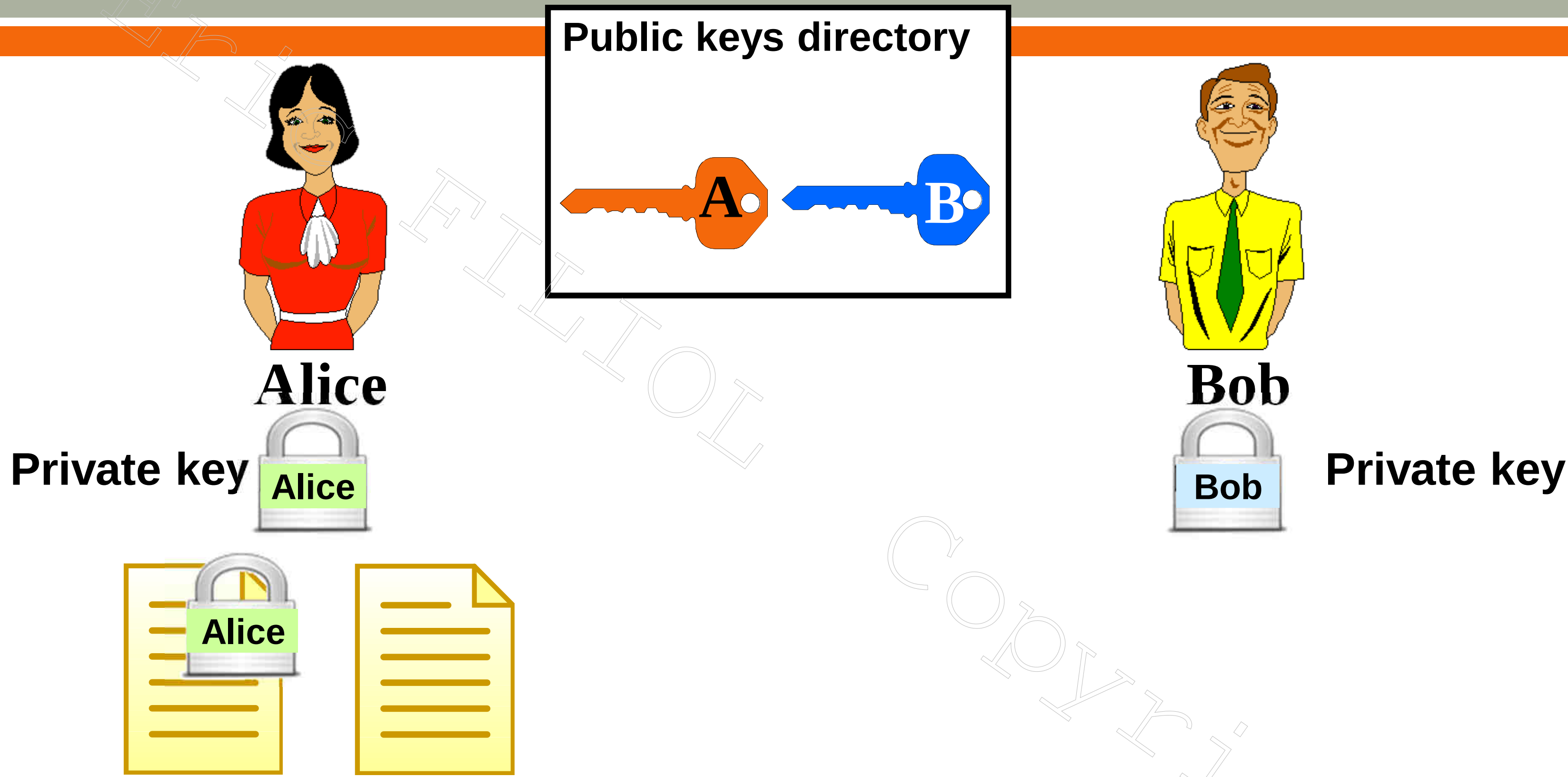
Digital Signature



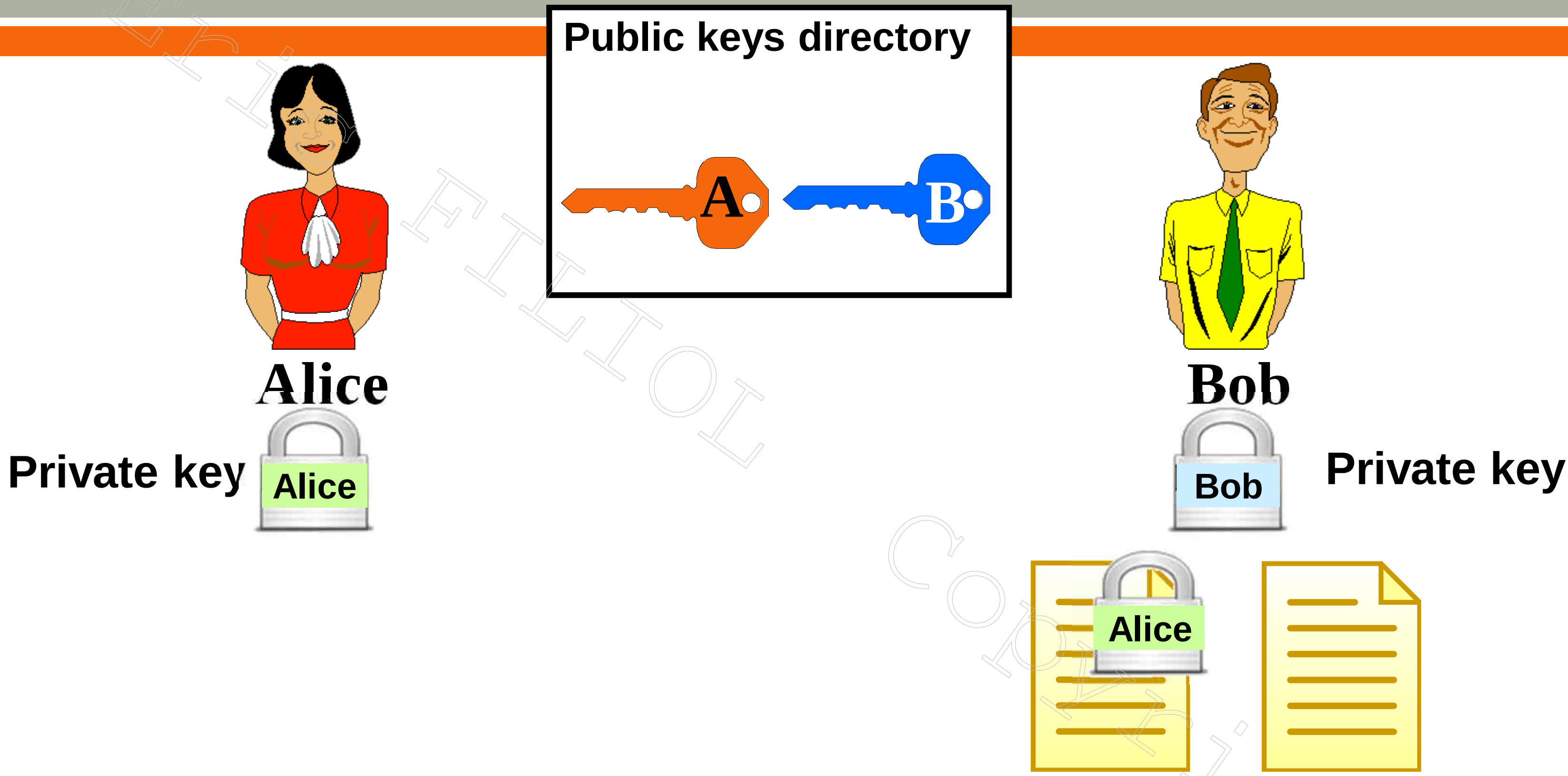
Digital Signature



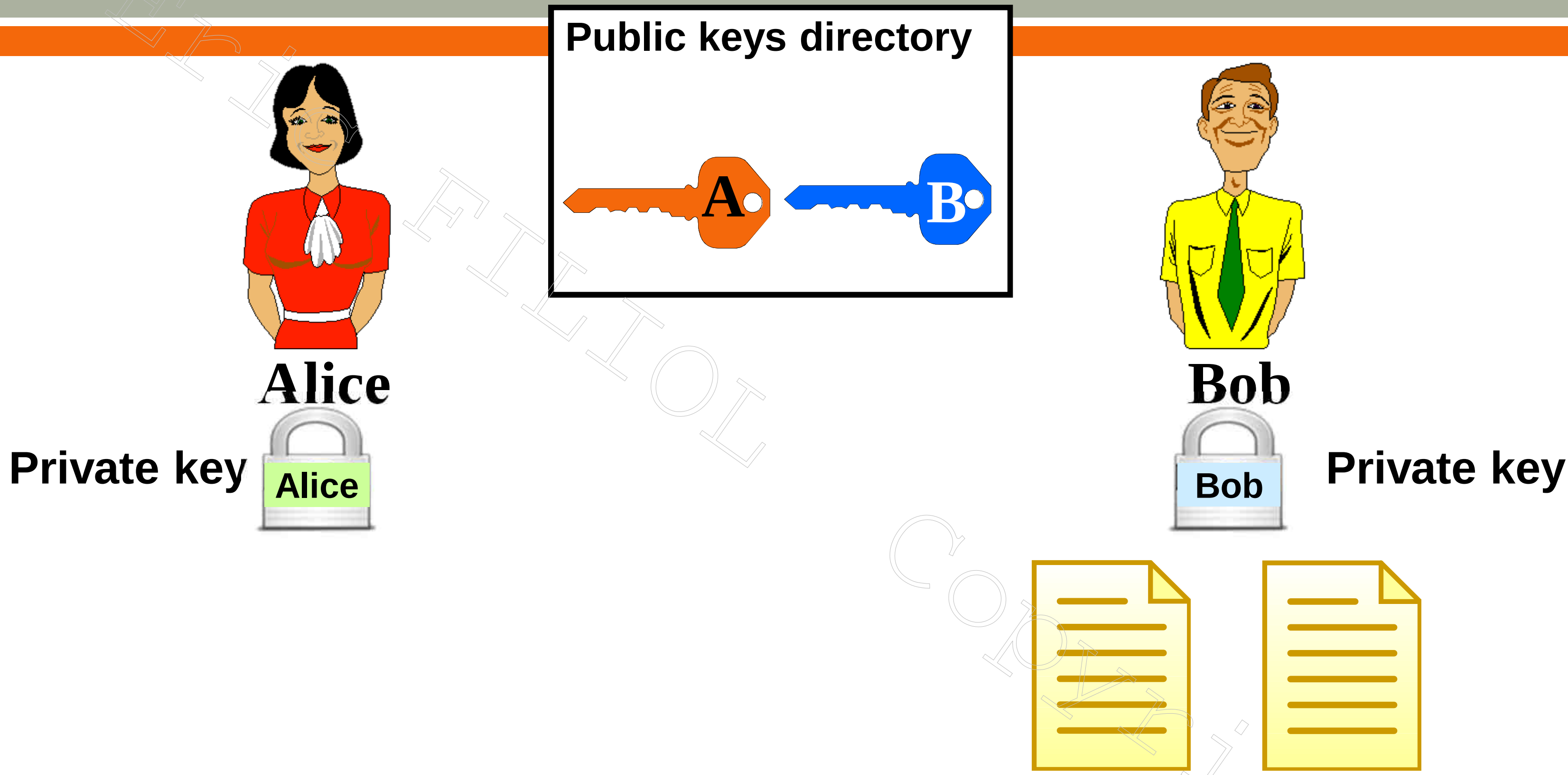
Digital Signature



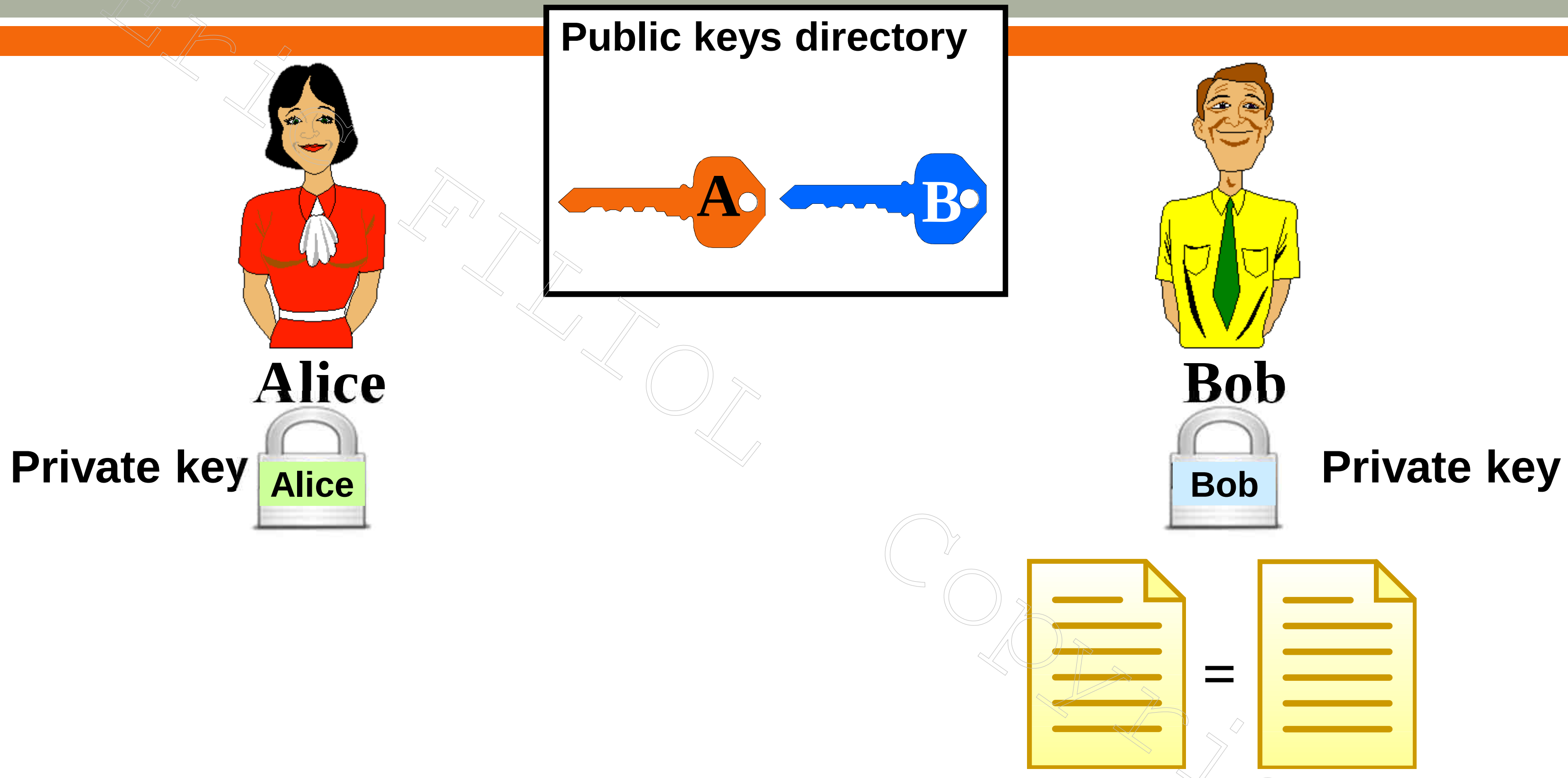
Digital Signature



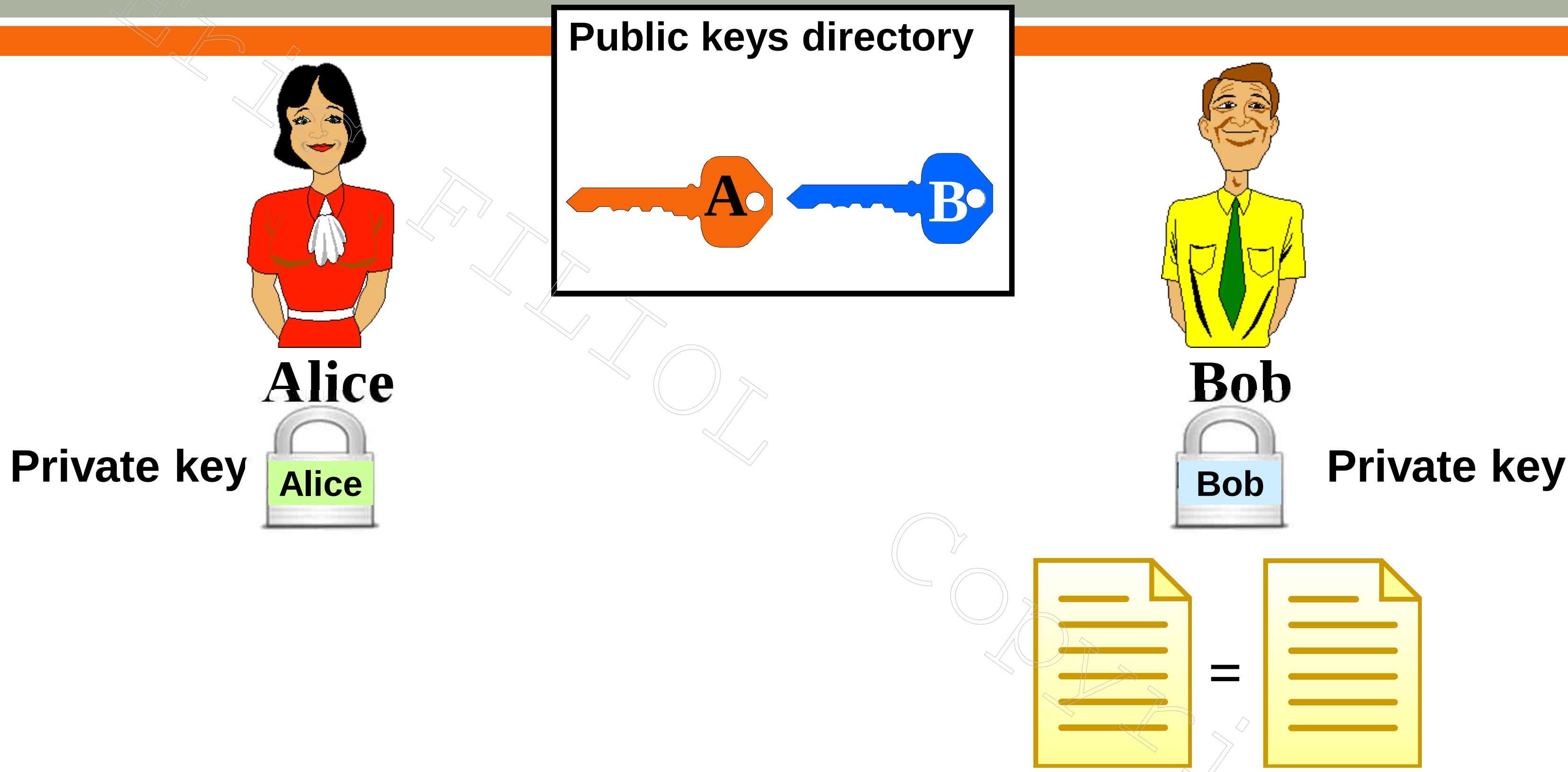
Digital Signature



Digital Signature



Digital Signature



Digital Signature

- To summarize:
  - We sign a copy of the message by using our own private key.
  - The digital signature is verified by using the related public key.

- Since the public is accessible to anyone, anyone can check and confirm the signature origin and validity.
- We use hash functions to speed up the process:
  - The hash value H(M) is signed
  - The recipient receives the signed hash, then check its validity.

Agenda

- Introduction
- Basic Terminology
- The History of Cryptology
- Cryptology : Threats and Solutions :
  - Encryption
  - Hash
  - Electronic signature
- Basic Knowledge on Cryptanalysis
- Conclusion

Crytographic Keys

- Key principle:

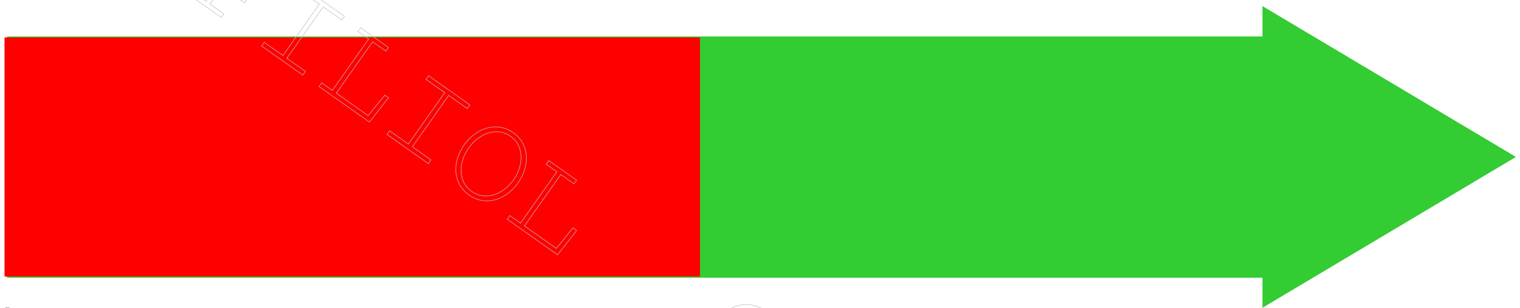
The cryptographic security must lie in the key secrecy and not in the algorithm secrecy (Kerckhoffs'laws – 1883)

- Key : secret quantity and parameter in a cryptographic algorithm

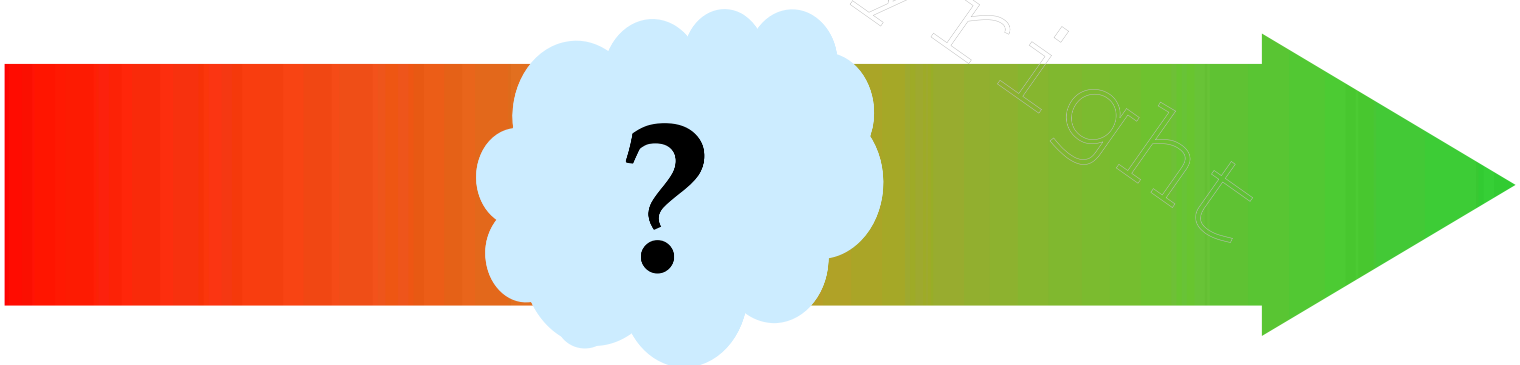
- Key features and properties
  - o Entropy : the amount of secret or uncertainty about the key
  - o Cryptoperiod : the operational timelife of a key

Crytographic Keys

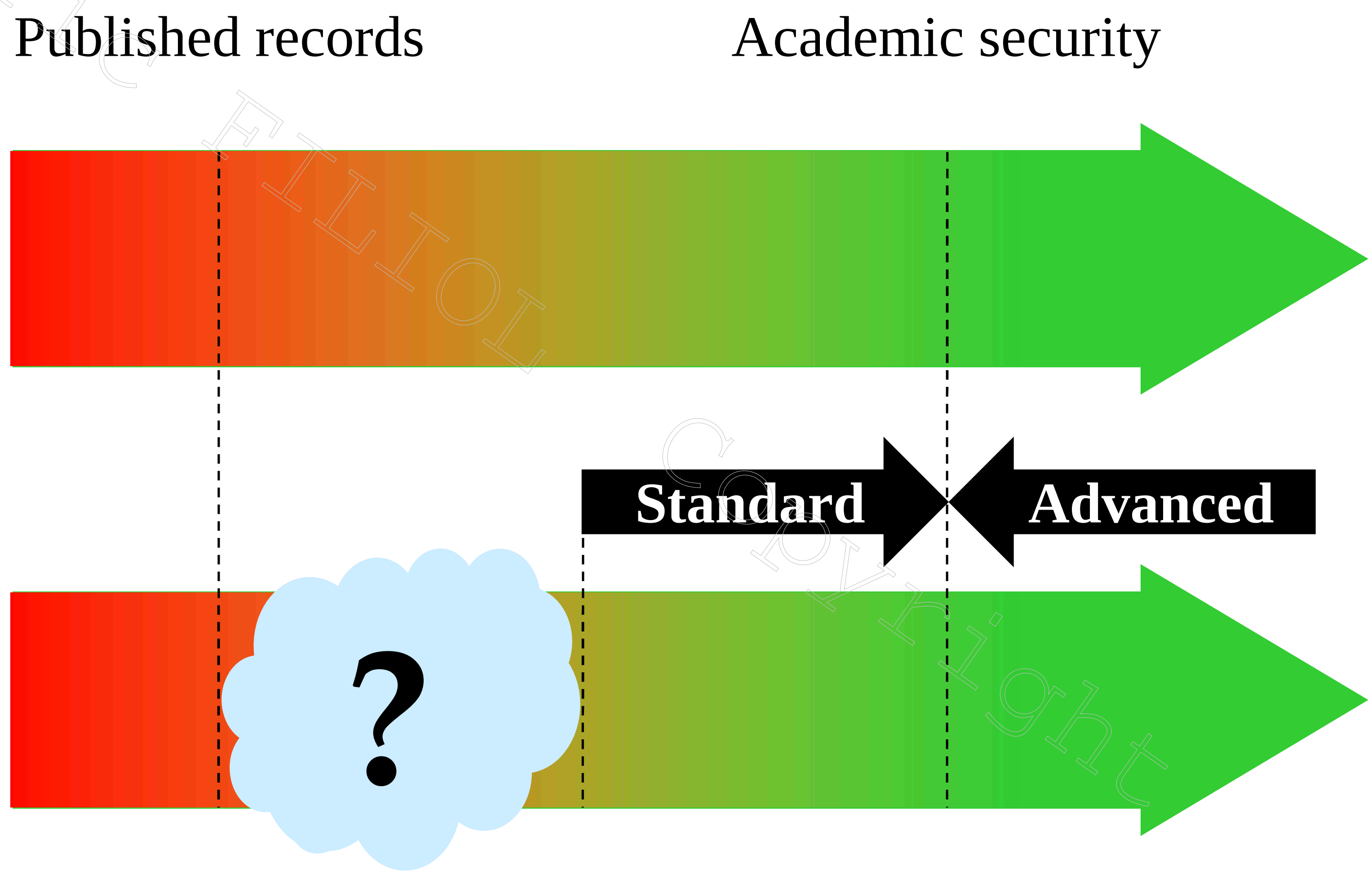
- Entropy :
  - Ideal view



  - Reality



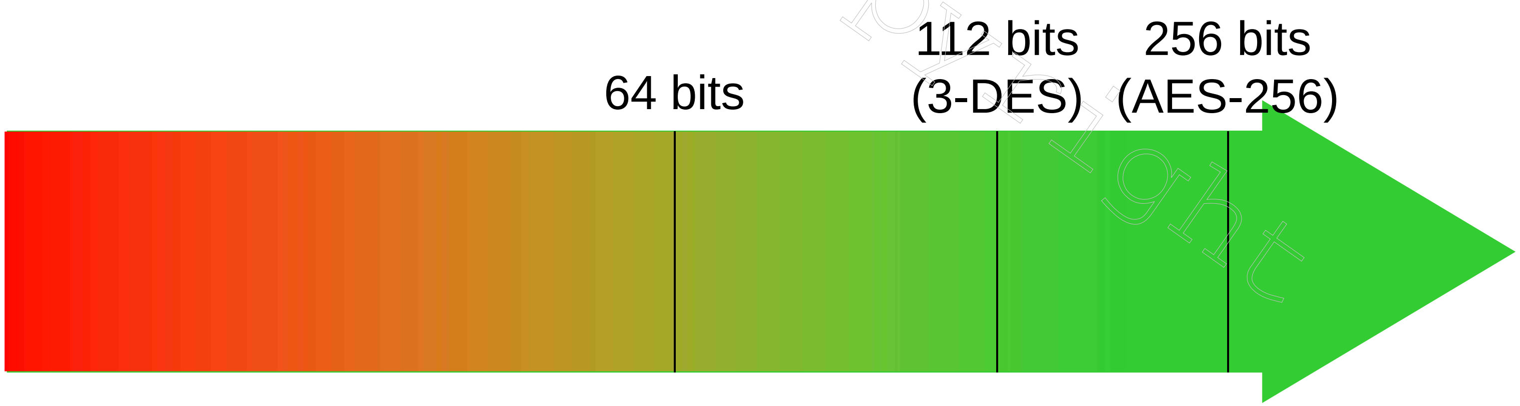
Crytographic Keys



Crytographic Keys

- To be more precise : symmetric encryption
  - 1980-90 :

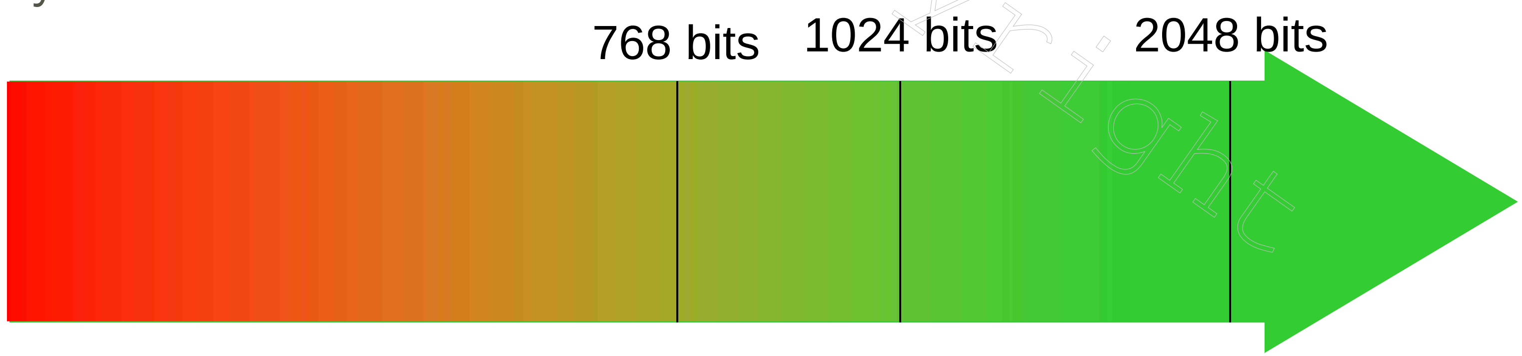
  - Today :



Crytographic Keys

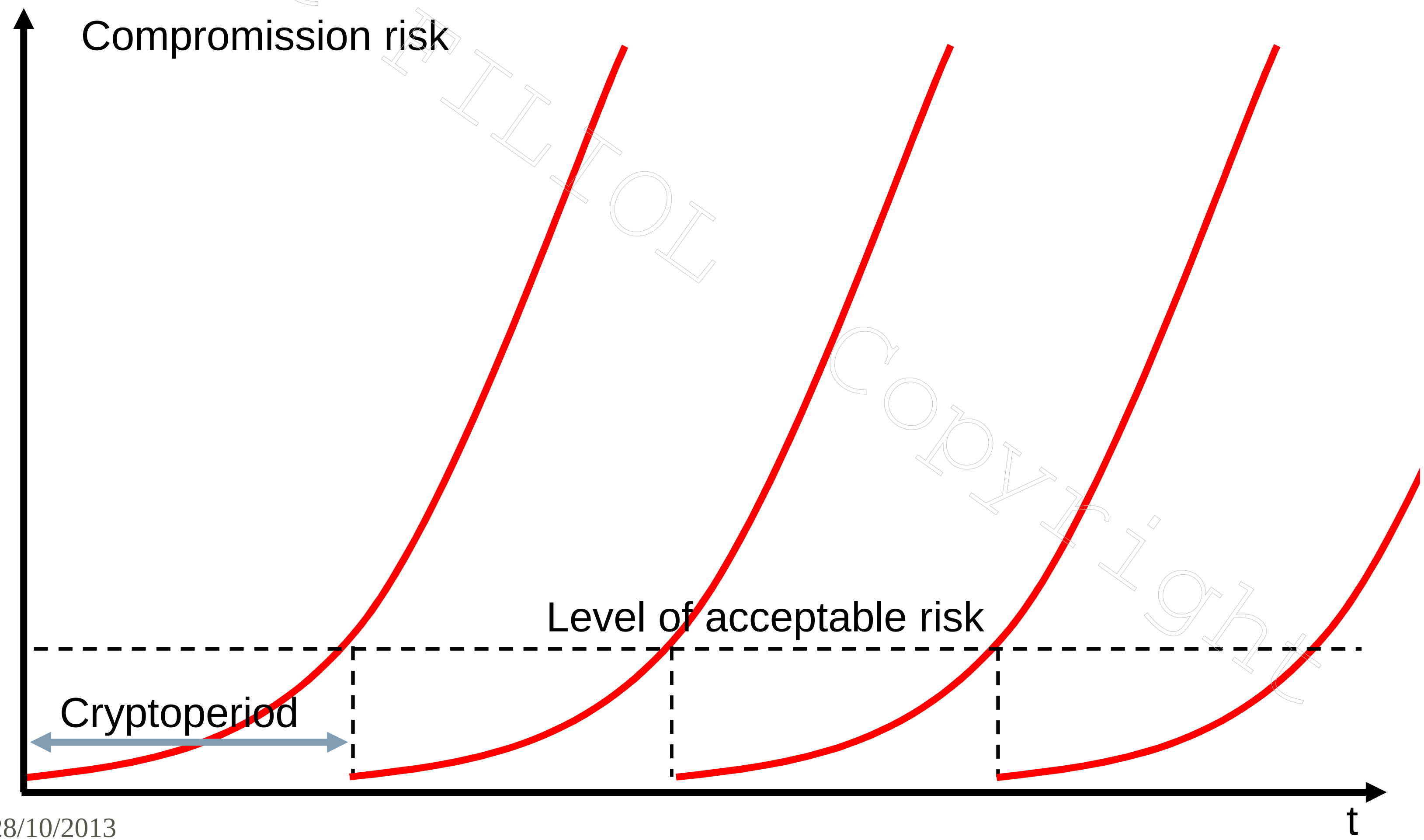
- To be more precise : asymmetric encryption
  - 1980-90 :

  - Today :



Crytographic Keys

- Cryptopériode



Cryptanalysis

- The security lies on the key secrecy only!
  - We always assume that the algorithm is known by the attacker.
  - We cannot of course limit this knowledege as much as possible

- Ciphertext-only attack:
  - The attacker has the ciphertext and wants to recover the plaintext and/or the secret key.
  - We use the underlying language redundancy (Shannon 2nd Theorem)
  - Exhaustive key search.

- Probable, known and chosen plaintext attacks
  - Limited operational scope beyond a few bytes of plaintext

Agenda

- Introduction
- Basic Terminology
- The History of Cryptology
- Cryptology : Threats and Solutions :
  - Encryption
  - Hash
  - Electronic signature
- Basic Knowledge on Cryptanalysis
- Conclusion

Conclusion

- Cryptology is THE critical dimension of IT security.
- If the scientific aspects are essential, implementation and management issues are even more essential
- Most of the standards we use are not ours
    - Still many uncertainty and lack of security proof

Bibliography

- David Kahn. *The Codebreakers* – The History of Secret Communication. McMillan Publishing
- Simon Singh. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Doubleday Publishing*
- *Eric Filiol. The Control of Technology by Nation State: Past, Present and Future - The Case of Cryptology and Information Security. Journal of Information Warfare, vol. 12, issue 3, October 2013.*
- *Menezes A. J., van Oorschott, P. C & Vanstone S. A. Handbook of Cryptography. CRC Press*