Cryptography
Lecture 1

Dr. Panagiotis Rizomiliotis
Assistant Professor

Dep. Of Informatics and Telematics
Harokopio University of Athens

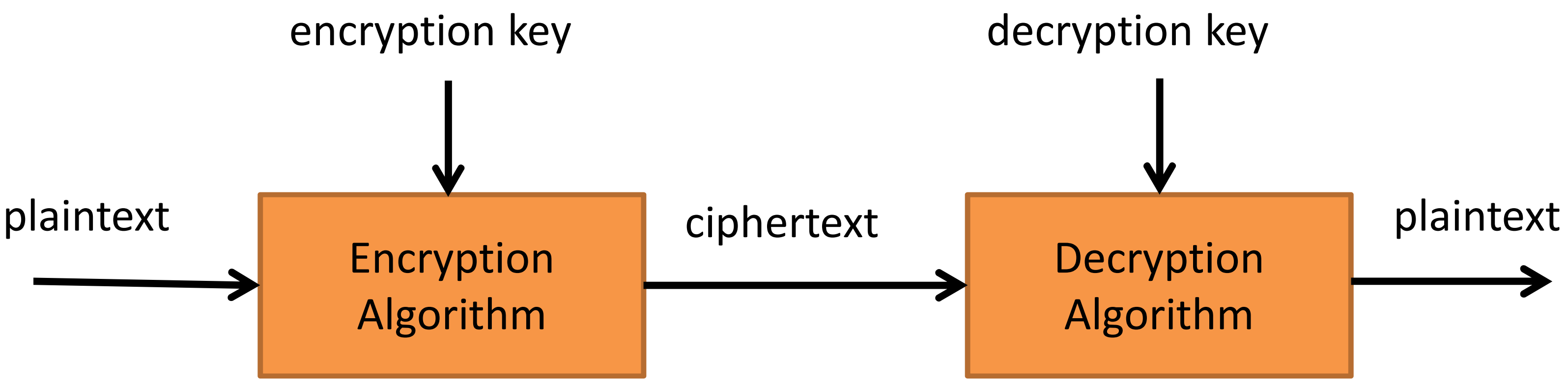
Agenda

- Introduction
- History of cryptography
- Crypto agenda

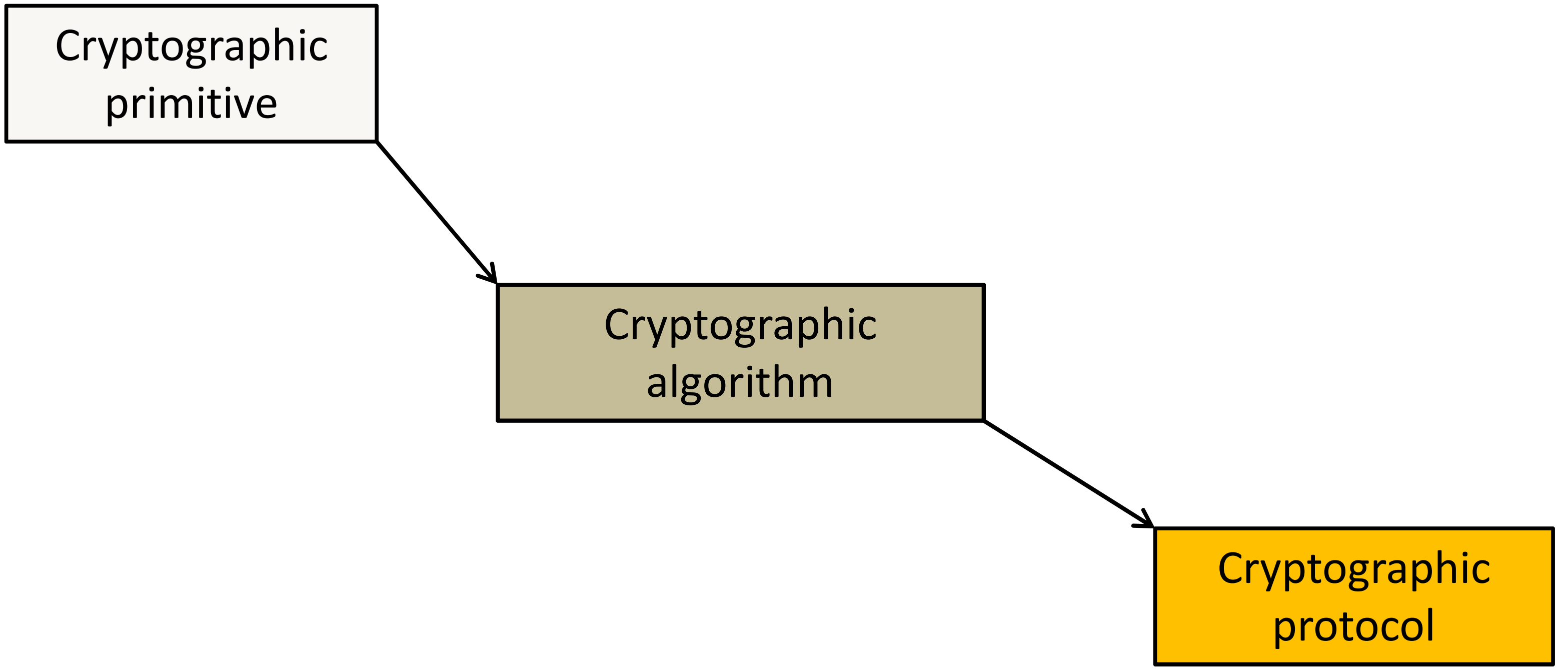
DEFINITIONS

- Cryptography
- Cryptanalysis
- Cryptology
- Cryptosystem

BASIC MODEL OF A CRYPTOSYSTEM



(MORE) DEFINITIONS



Cryptographic primitive

Cryptographic algorithm

Cryptographic protocol

TRADITIONAL SECURITY GOALS

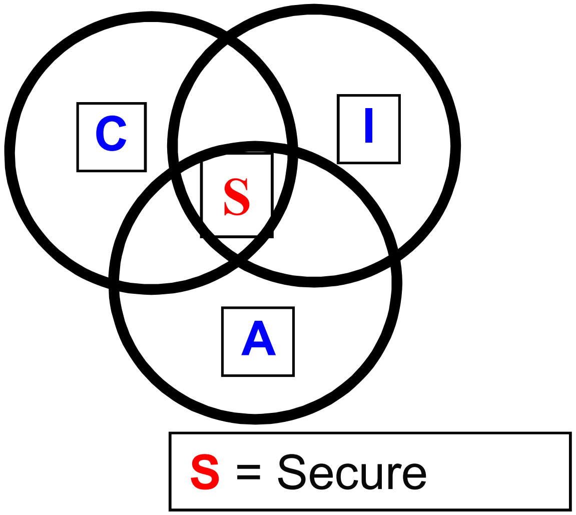
✓ Confidentiality

✓ Data Integrity

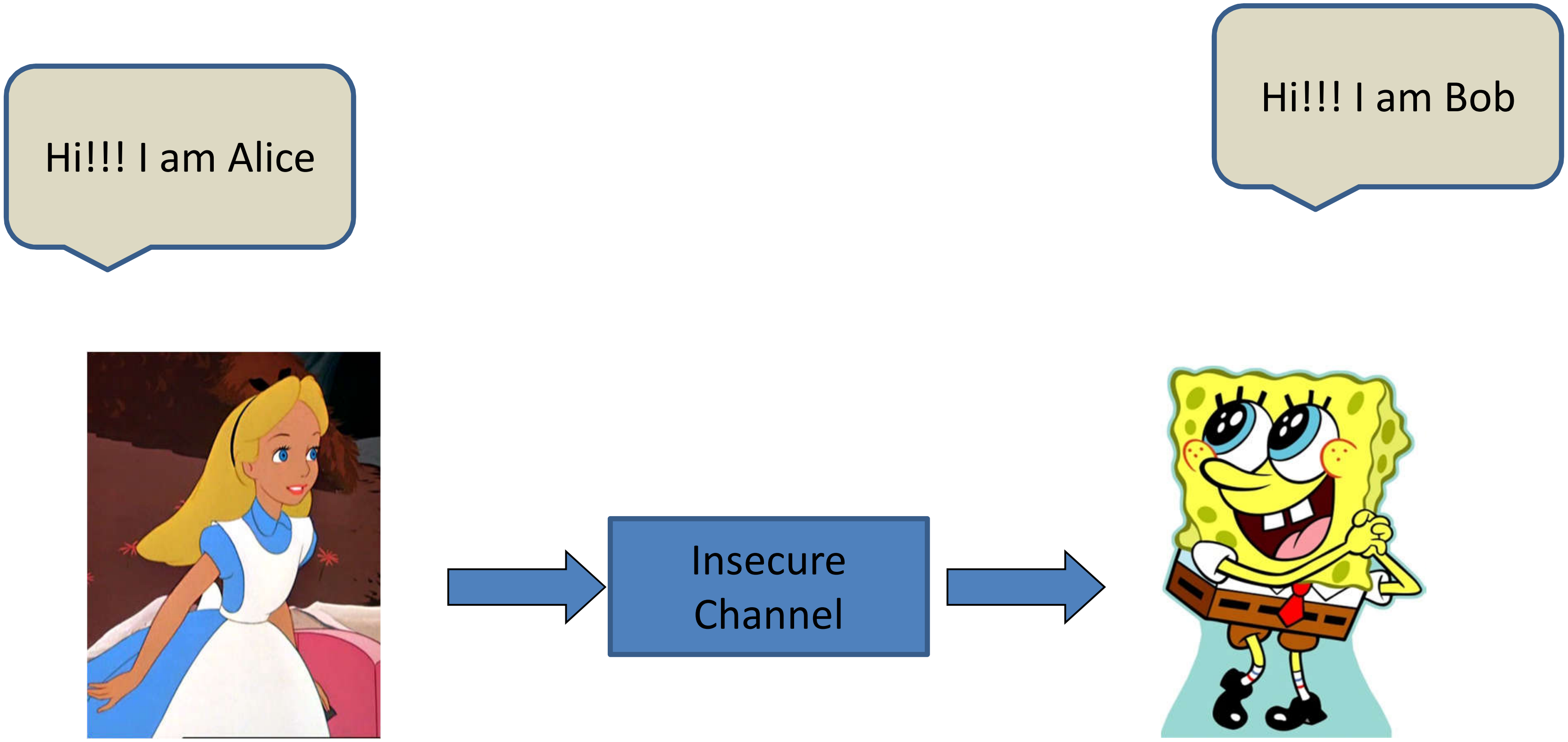
✓ Data origin authentication/

- entity authentication

- **More…**
- Authorization
- Privacy
- Non-repudiation
- …



SECURITY GOALS

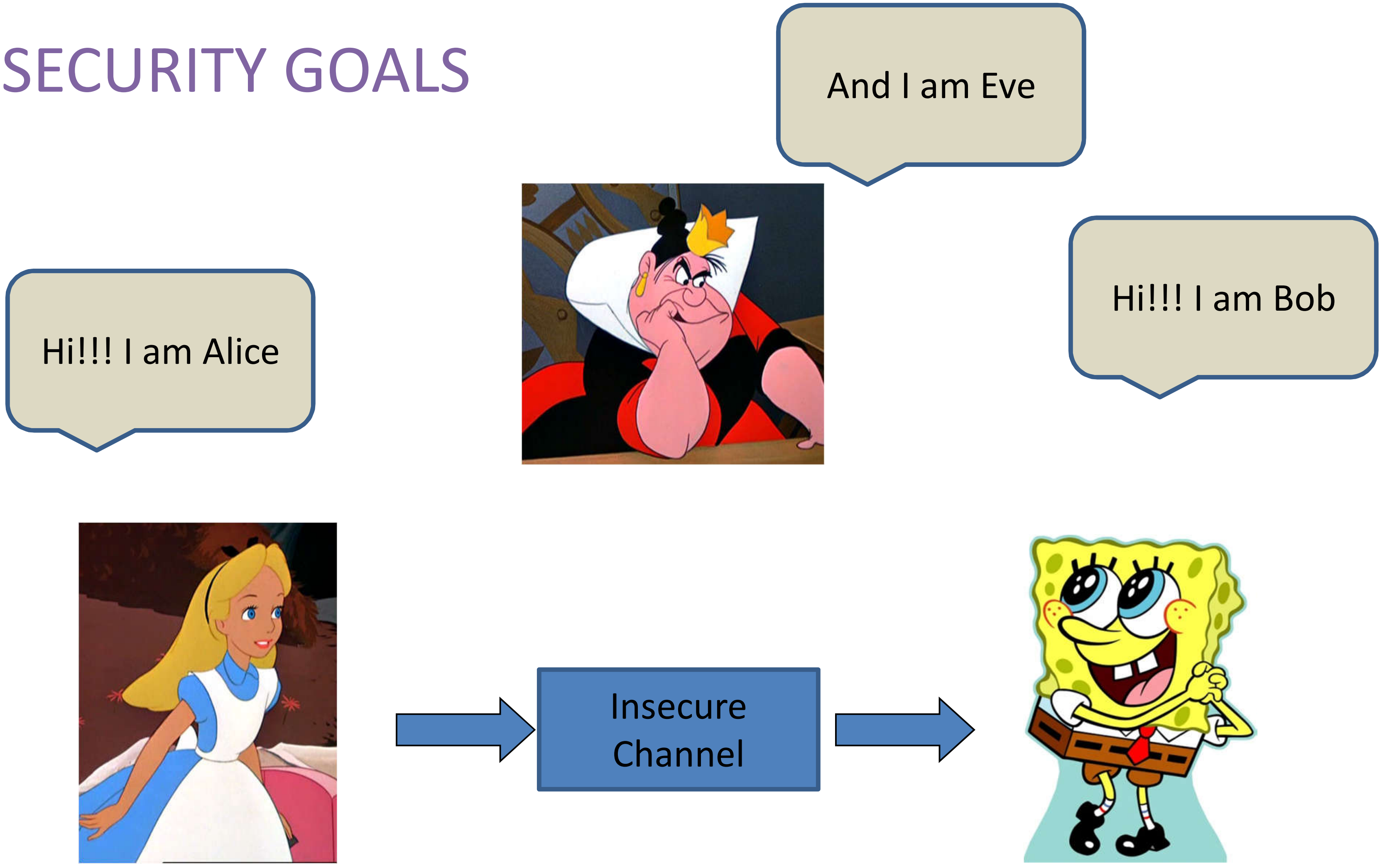


Hi!!! I am Alice

Hi!!! I am Bob

Insecure Channel

SECURITY GOALS



And I am Eve

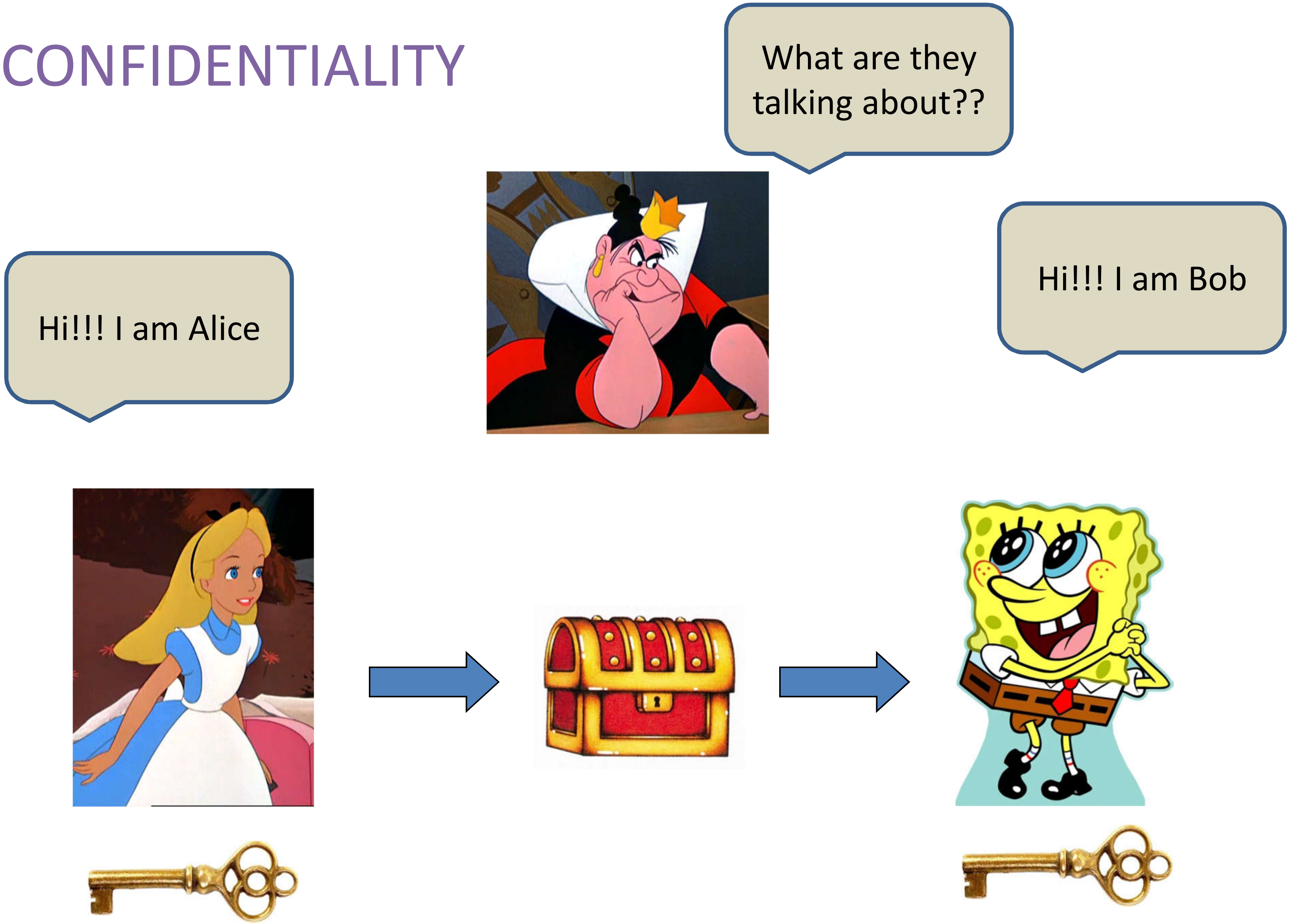
Hi!!! I am Alice

Hi!!! I am Bob

Insecure Channel

This is an attack model…

CONFIDENTIALITY

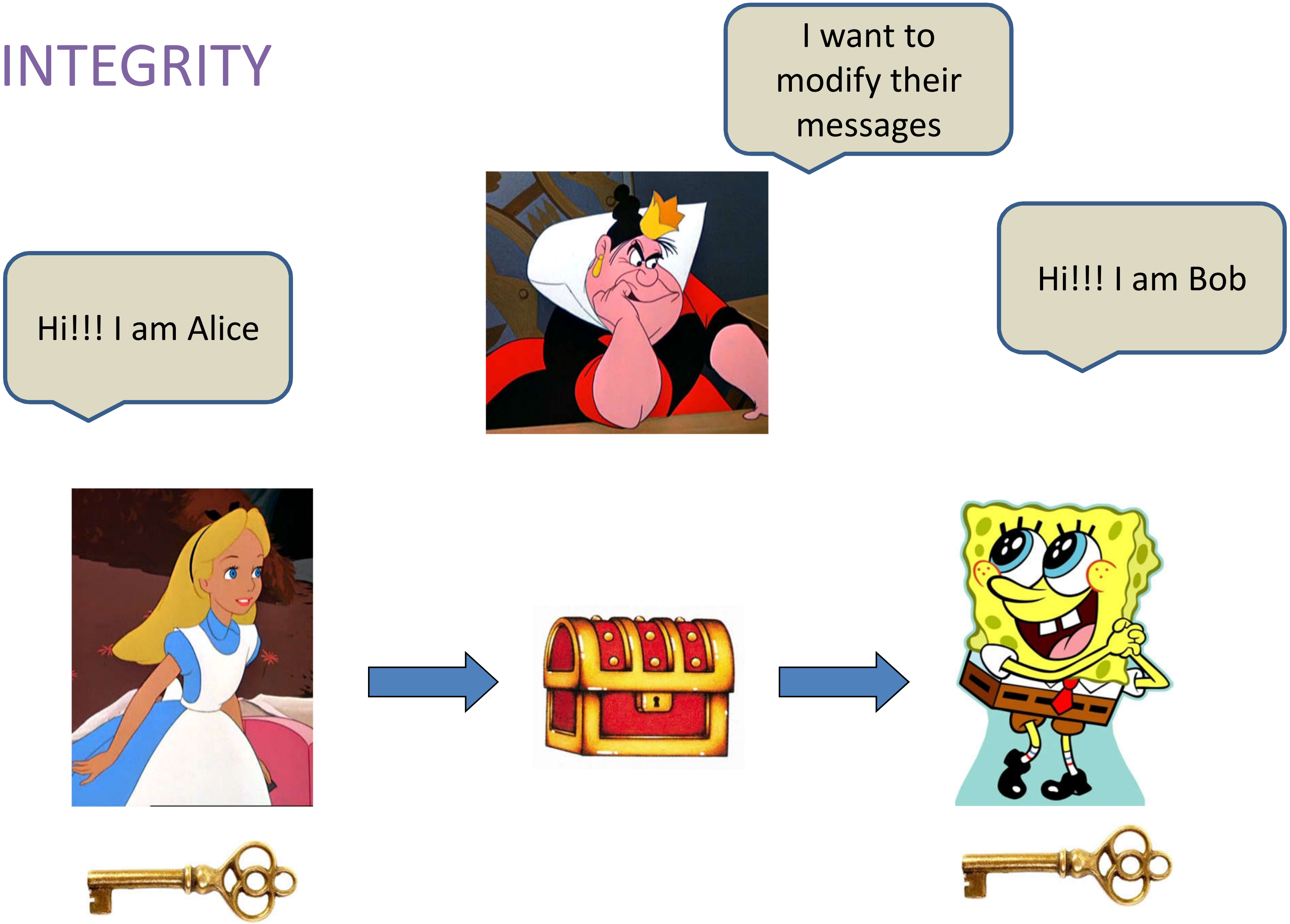


What are they talking about??

Hi!!! I am Alice

Hi!!! I am Bob

INTEGRITY

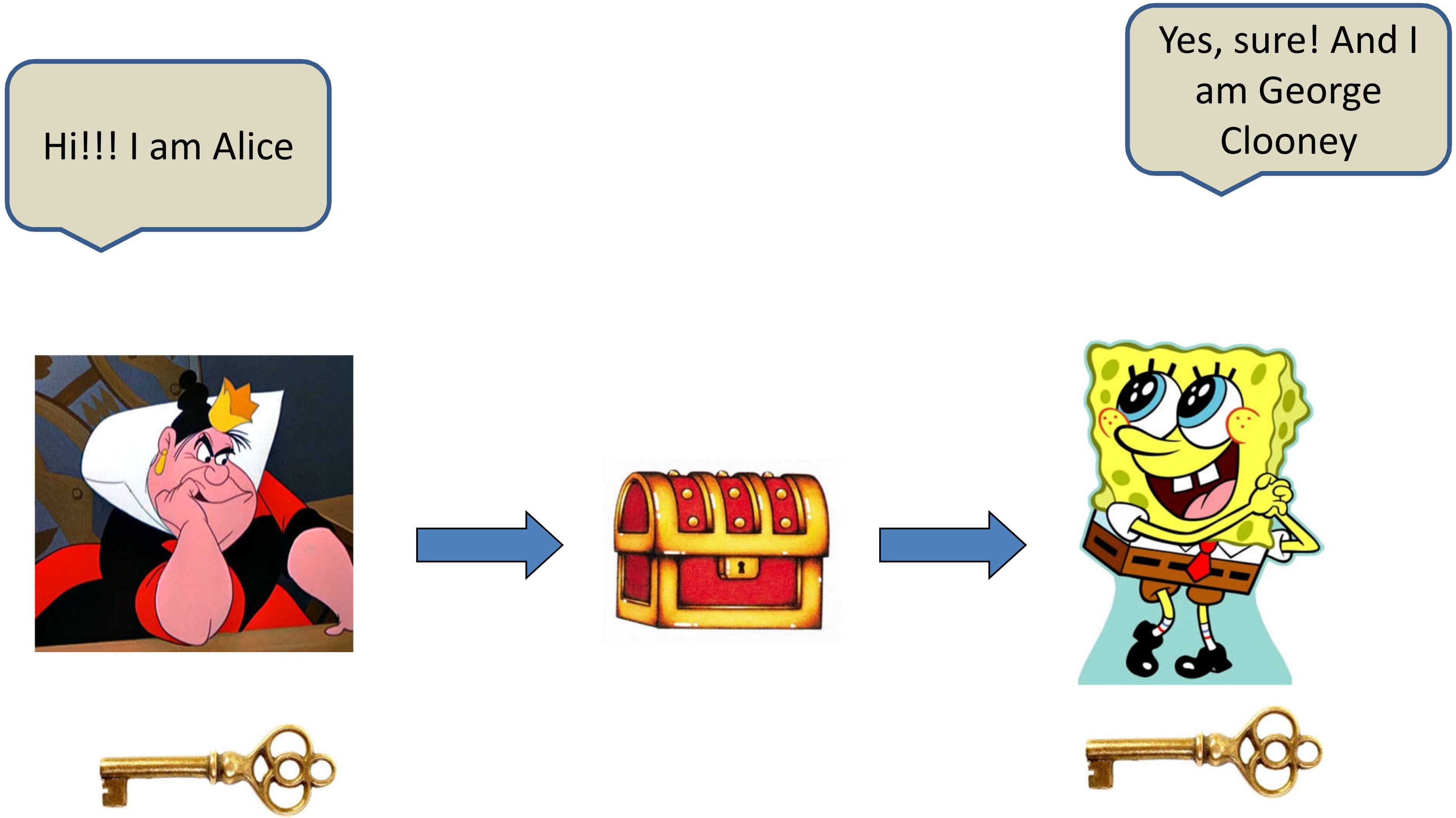


I want to modify their messages

Hi!!! I am Alice

Hi!!! I am Bob

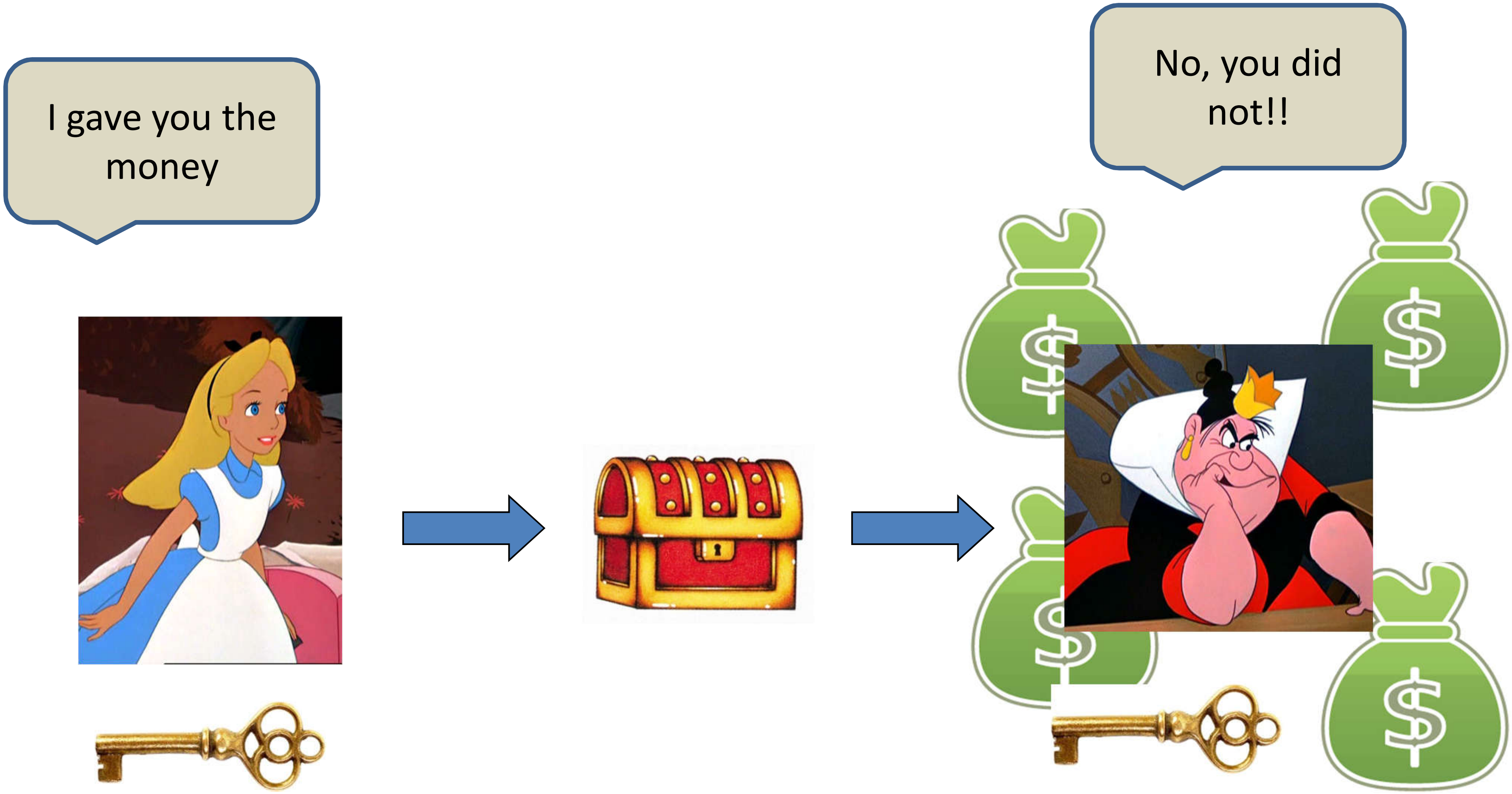
AUTHENTICATION



Hi!!! I am Alice

Yes, sure! And I am George Clooney

NON – REPUDIATION



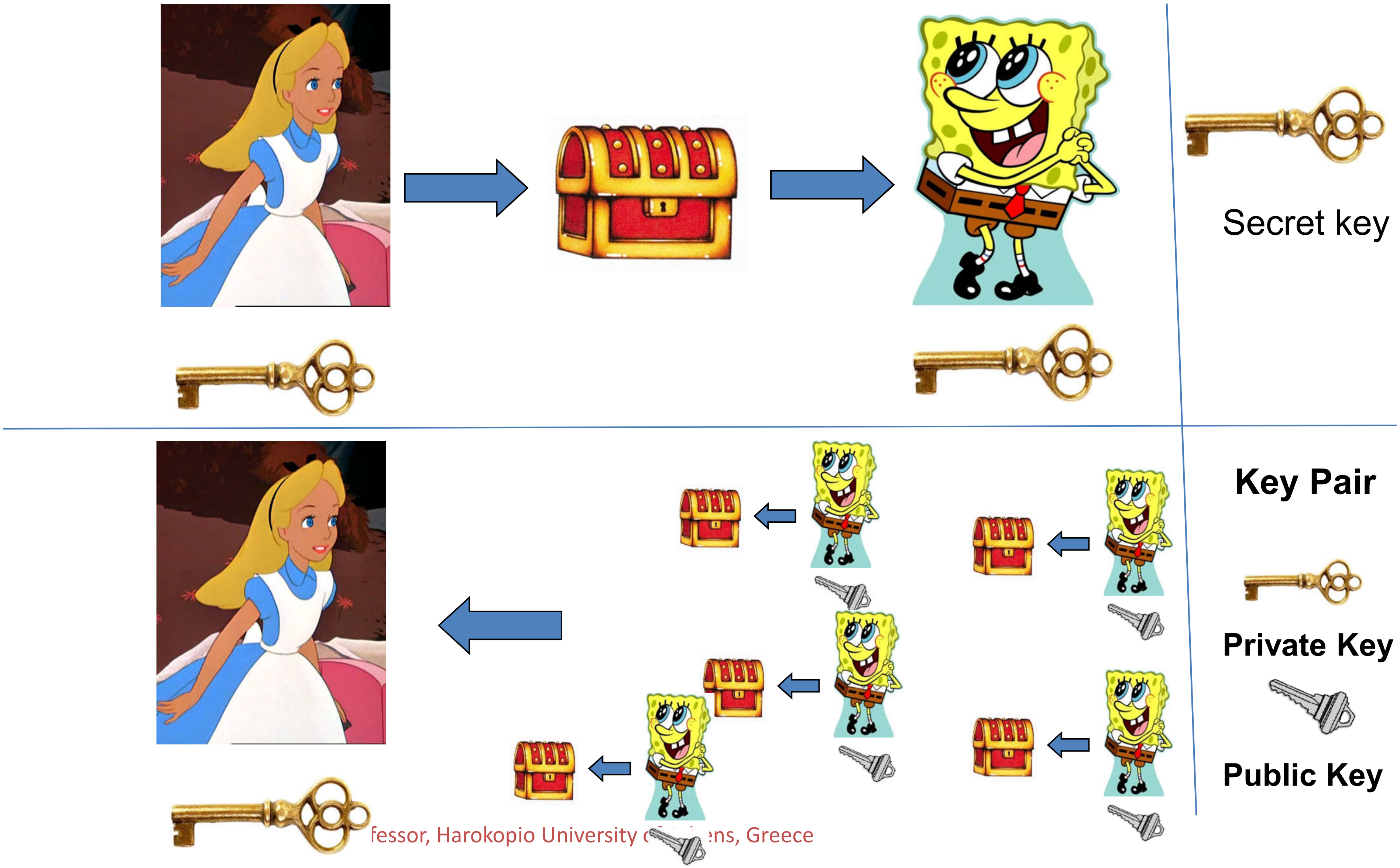
TYPES OF CRYPTOSYSTEMS

- **Two types of cryptosystems**

1. Symmetric key

2. Asymmetric or public key

SYMMETRIC KEY VS PUBLIC KEY



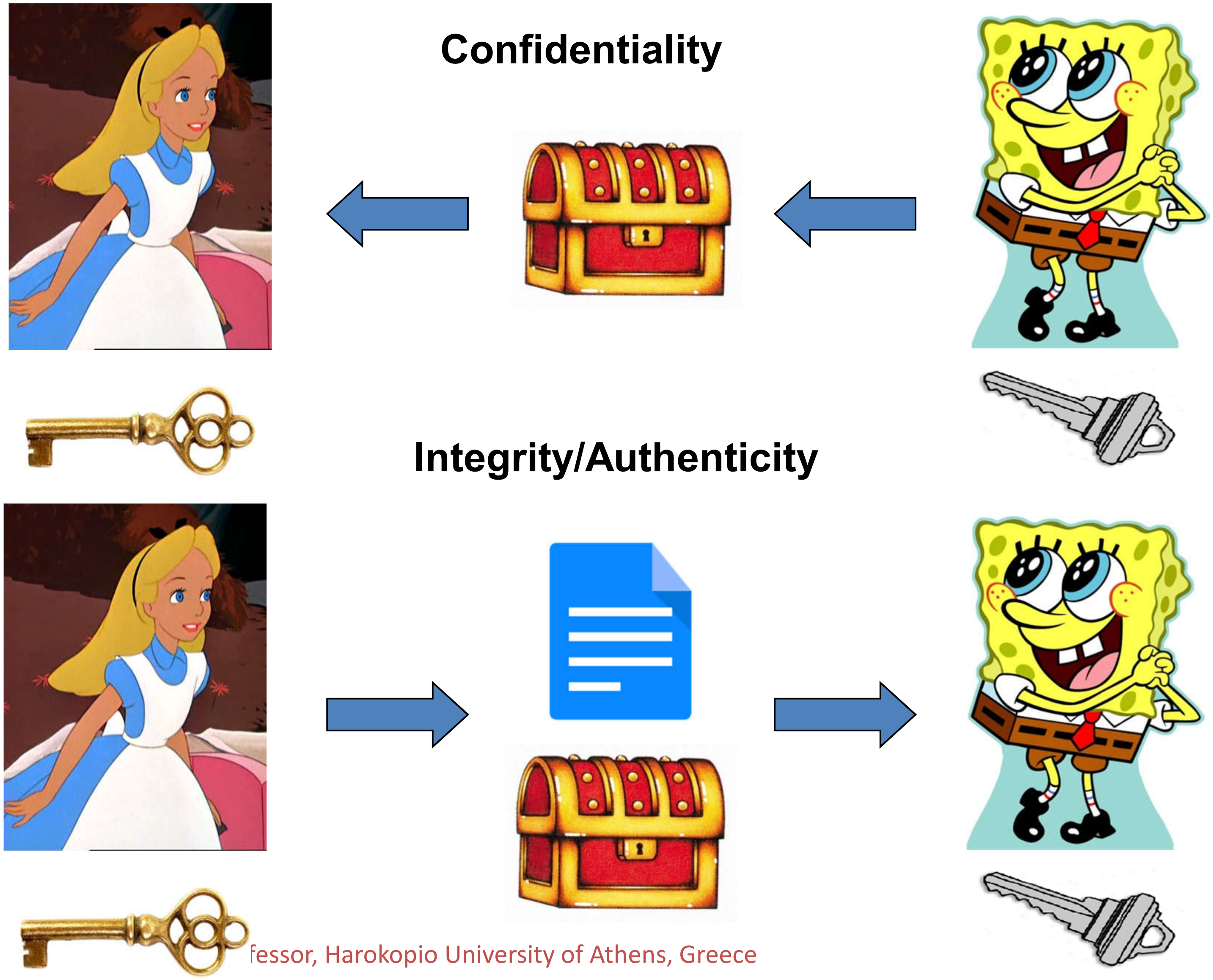
Secret key

Key Pair

Private Key

Public Key

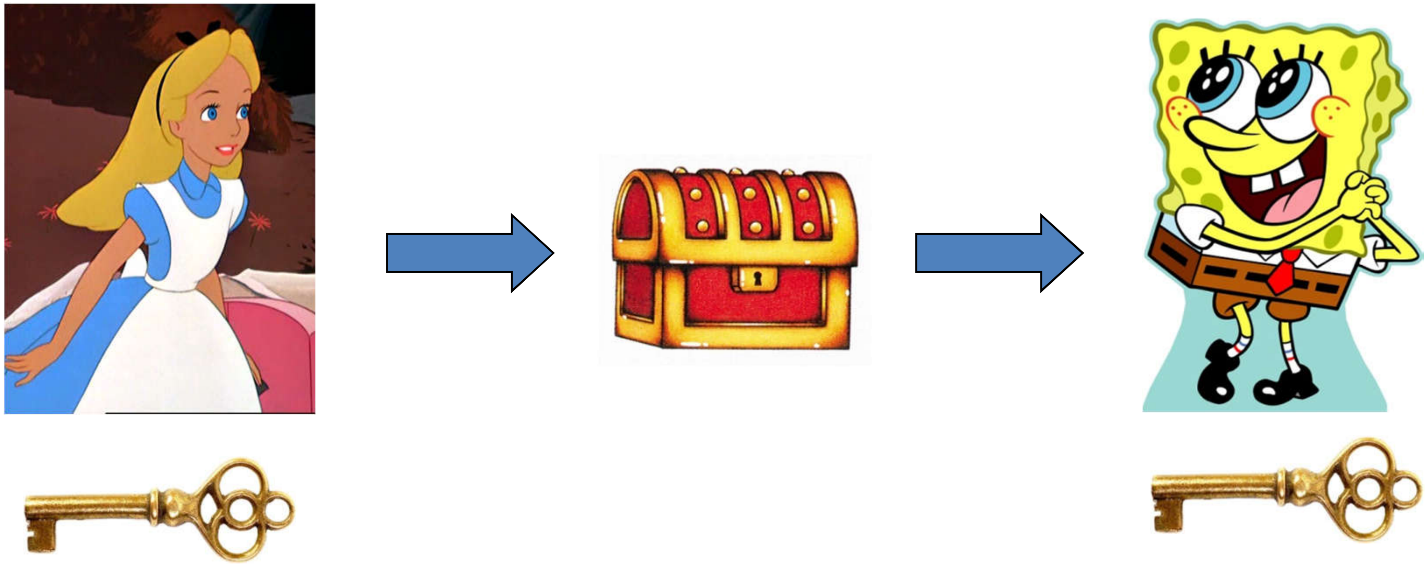
ASYMMETRIC KEY (PUBLIC KEY)



Confidentiality

Integrity/Authenticity

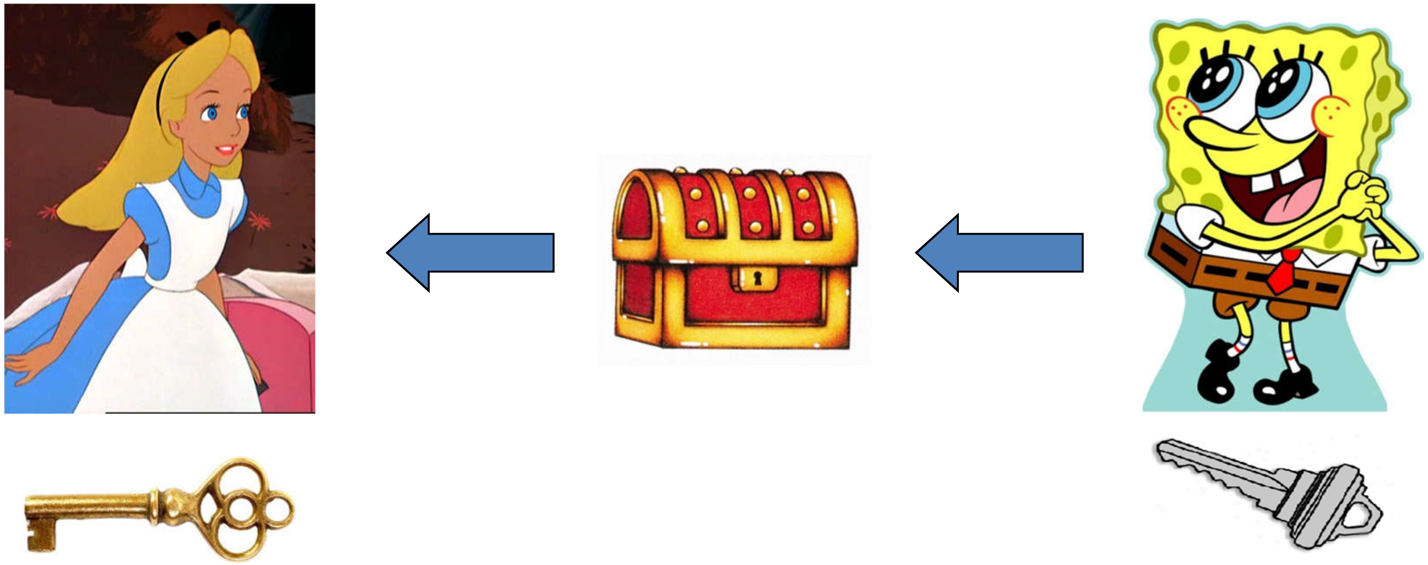
SYMMETRIC KEY – KEY EXCHANGE

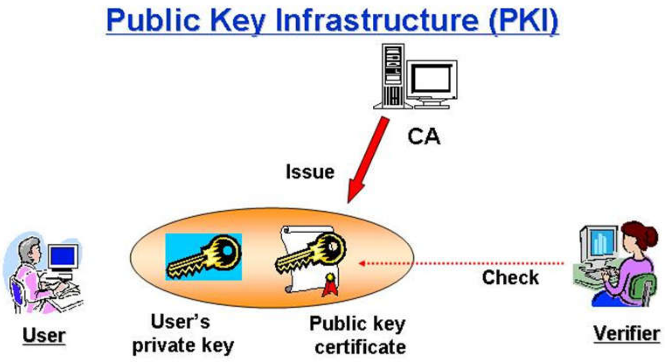


Meeting place

Trusted Third Party (TTP)

PUBLIC KEY – KEY EXCHANGE





Public key infrastructure (PKI)

KNOWLEDGE OF ENCRYPTION ALGORITHMS

- **Publicly known algorithms**
- transparency
- Interoperability
- Usually more secure

- **Proprietary algorithms**
- Used only in closed environments

AUGUSTE KERCKHOFFS

- A cryptosystem should not be required to be secret in order to be secure.

(Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs von Nieuwenhof)

TYPE OF SECURITY

- **Unconditional security**

  No assumptions on the adversary

- **Computational security**

  Assumptions on the resources of the adversary

  - Time
  - Power
  - Memory
  - Data

PRELIMINARIES

- **Modern cryptography is based on a gap between**

efficient algorithms for encryption for the legitimate users

versus the computational infeasibility of decryption for the adversary

- **Requires that we have available primitives with certain special computational hardness properties.**
-

SECURITY DEFINITIONS

- Define the attack scenario
- Define the adversary (computational power, etc)
- Define the security goal (confidentiality of data)

- There are MANY DEFINITIONS!!!

ADVERSARY MODEL

- **Passive**

➢ Usually an eavesdropper

➢ Honest but curious

- **Active**

➢ She can modify the messages

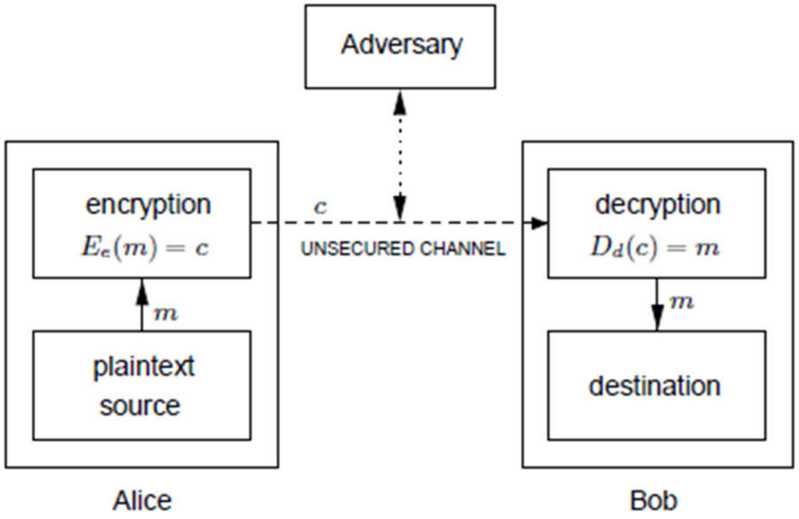
➢ more powerful adversary

➢ can request a polynomial number of ciphertexts to be decrypted for him

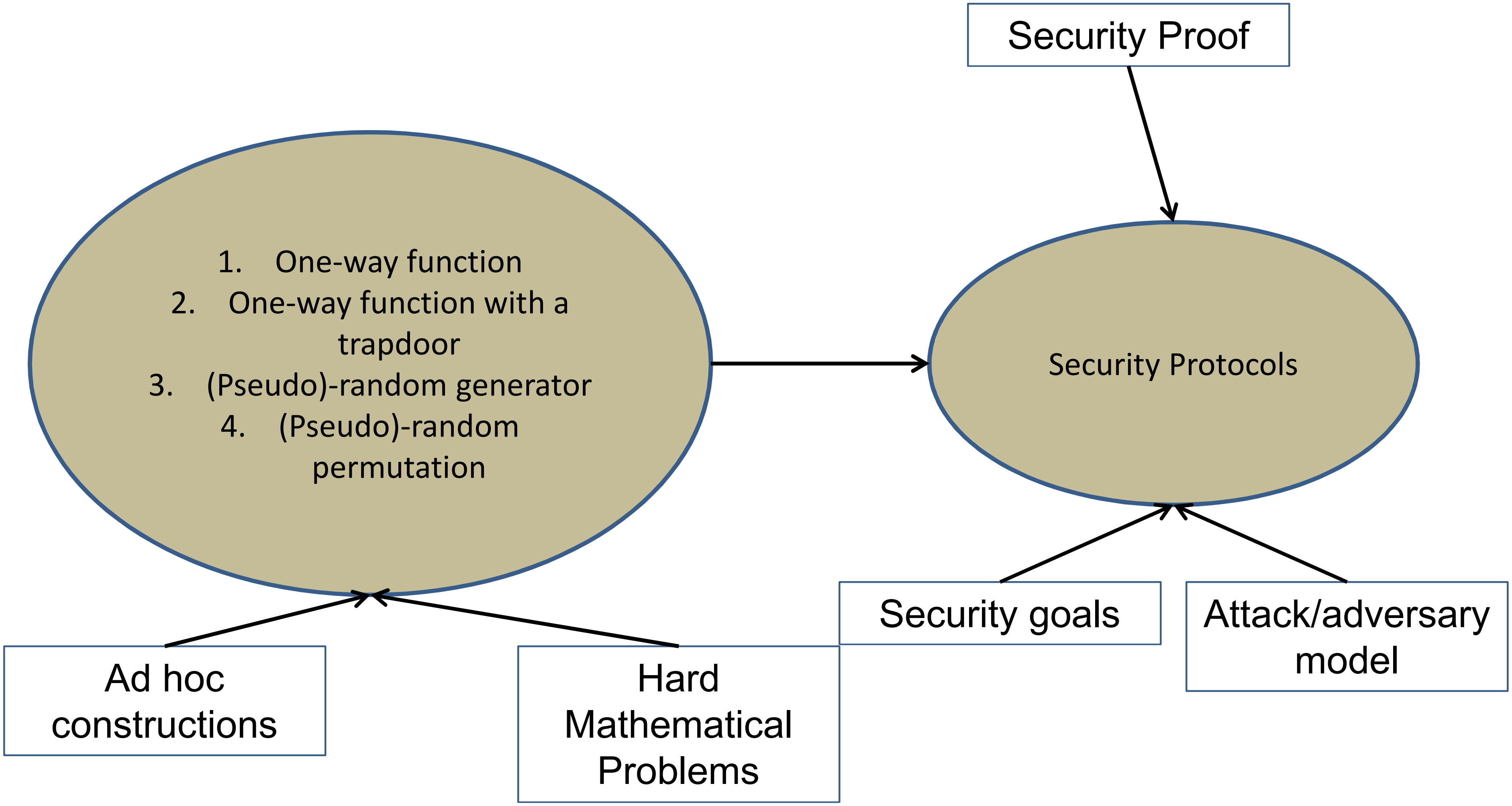
➢ intercept messages being transmitted from sender to receiver and either stop their delivery all together or alter them in some way

THEORETICAL ATTACK SCENARIOS

- 1) Ciphertext-only attack
- 2) Known-plaintext attack
- 3) Chosen-plaintext attack (CPA)
- 4) Adaptive chosen-plaintext attack
- 5) Chosen-ciphertext attack (CCA)
- 6) Adaptive chosen-ciphertext attack



BASIC STEPS



1. One-way function
2. One-way function with a trapdoor
3. (Pseudo)-random generator
4. (Pseudo)-random permutation

Security Protocols

Security Proof

Ad hoc constructions

Hard Mathematical Problems

Security goals

Attack/adversary model

Assistant Professor, Harokopio University of Athens, Greece

WHEN CRYPTOGRAPHY IS ‘BROKEN’?

- **When there is an attack that violates one of the security goals**
- **The attack is more efficient than the security parameter.**
- **Never assume that an algorithm or protocol can offer more than it was designed for.**
-
- **It must be evaluated first!**

CLASSES OF ATTACKS

1. **Generic attacks**
- key guessing (exhaustive search)
2. **Primitive specific**
3. **Algorithm specific**
4. **Side-channel attack**
- Bad implementations

EXHAUSTIVE SEARCH

- ✓ Also known as brute force
- ✓ Try to guess the key
- ✓ This attack always exists

- ➢ There are trade-offs between real-time and precomputation trade-off based on the birthday paradox

- ➢ You can avoid the attack by increasing the key space (key length)

- ➢ Modern algorithms have key length at least 128 bits.

- ➢ Top secret applications need 256 bits security

KEY SIZE

- ✓ How many binary keys of length 256 are there?
- ✓ Key space = 2^{256}

- ✓ How big is that?
- ✓ Approximately, 3.31 x 10^{56}.

- ✓ This is roughly equal to the number of atoms in the universe!

- ✓ The Sunway TaihuLight in China is capable of a peak speed of 93.02 petaflops.
- ✓ That means, it needs 885 quadrillion years to brute force a 128-bit AES key.

PRACTICAL VS THEORETICAL ATTACKS

- **Real world attacks**
- Exploit weaknesses of a real system and violate security goals

- **Theoretical (or academic) attacks**
- An attack that it is more efficient than the alleged bound, but still far from practical

PRACTICAL VS THEORETICAL ATTACKS

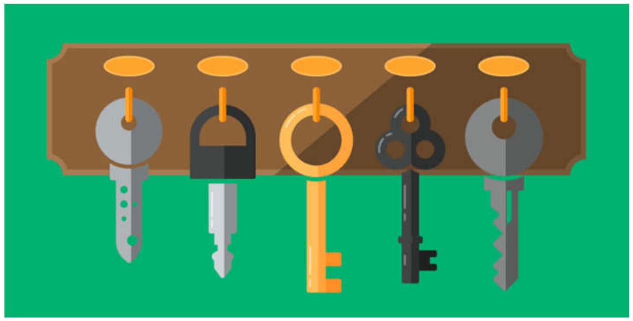
- Example:

- Theoretical:
- there is an attack against AES that allows to crack the algorithm four times faster than was possible previously.

- In practice:
- If you have a trillion machines, that each could test a billion keys per second, it would take more than two billion years to recover an AES-128 key.

WHAT IS THE BEST WE CAN HOPE FOR

1. The primitive is solid
2. The algorithm and the protocol are secure
3. The implementation flawless

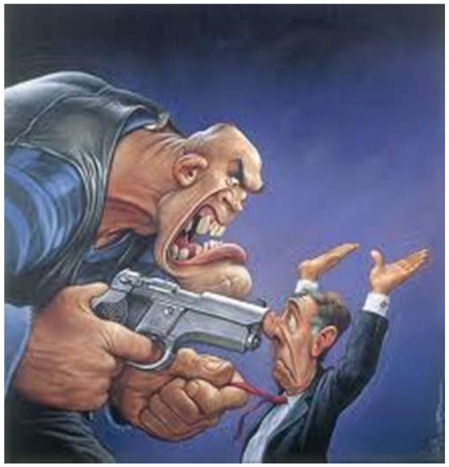


- Then, it is all about the secret keys.

- Manage the circle of life of a key
- (generate the key, establish, use, store, delete/archive)

- Much more difficult than it sounds!!

OTHER ATTACKS…



©2001 HowStuffWorks

DROPS OF CRYPTOGRAPHIC HISTORY

Assistant Professor, Harokopio University of
Athens, Greece

A VERY OLD STORY…

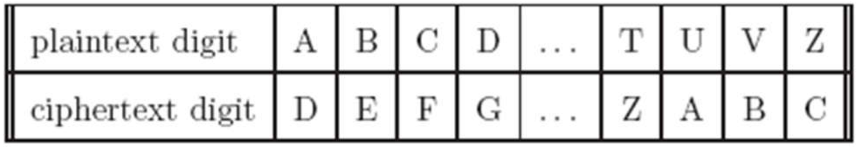
- We can identify the 4 main historical periods:

1. 4000 BC until WW II
2. WW II until the 70s
3. The 70s until today
4. The Quantum Computing Era

FIRST PERIOD – HIGHLIGHTS!

FIRST PERIOD – HIGHLIGHTS!

- **Caesar's Cipher**



plaintext digit	A	B	C	D	...	T	U	V	Z
ciphertext digit	D	E	F	G	...	Z	A	B	C

- A substitution cipher
- Symmetric
- Secret key: the number of shifts. Naively always equal to 3. The size of keyspace is 26.
- Plaintext/Ciphertext: the letters of the alphabet from A to Z.

Several variations of the cipher.

- Simple substitution
- Polyalphabetic substitution

FIRST PERIOD – HIGHLIGHTS!

- **Cryptosystem – simple substitution**

- Secret key: The size of keyspace is 26! (factorial) = 4x10^{26}
- n!=n x (n-1) x …x 1

- *Example*
- plain alphabet : a b c d e f g h I j k l m n o p q r s t u v w x y z
- cipher alphabet: p h q g I u m e a y l n o f d x j k r c v s t z w b

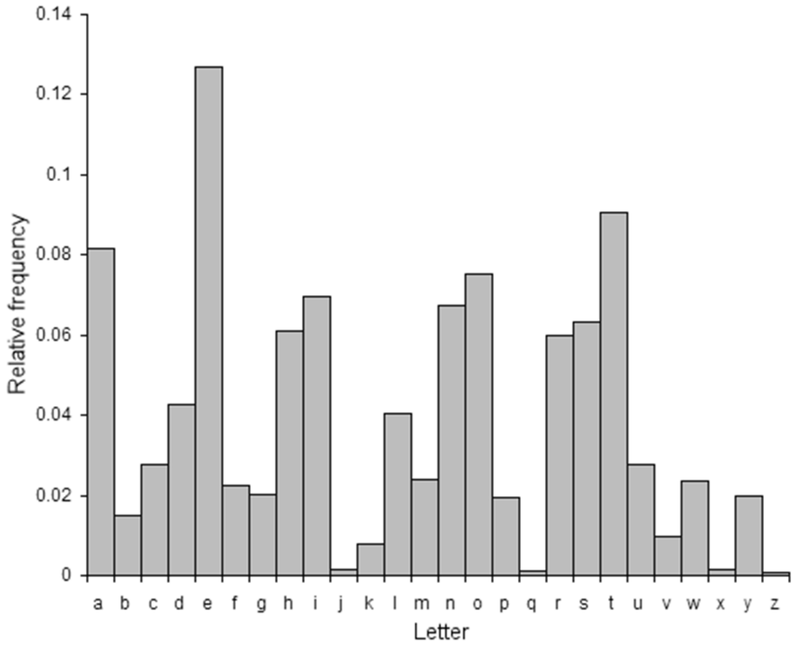
- plaintext: defend the east wall of the castle
- ciphertext: giuifg cei iprc tpnn du cei qprcni

SUBSTITUTION CIPHER CRYPTANALYSIS

- **Frequency analysis**

- The ciphertext does not hide the statistics of plaintext

http://substitution.webmasters.sk/simple-substitution-cipher.php



Letter average frequency

EXAMPLE (TEXT FROM THE BOOK “AROUND THE WORLD IN 80 DAYS”)

- During his brief interview with Mr. Fogg, Passepartout had been carefully observing him. He appeared to be a man about forty years of age, with fine, handsome features, and a tall, well-shaped figure; his hair and whiskers were light, his forehead compact and unwrinkled, his face rather pale, his teeth magnificent. His countenance possessed in the highest degree what physiognomists call ‘repose in action,’a quality of those who act rather than talk. Calm and phlegmatic, with a clear eye, Mr. Fogg seemed a perfect type ofthat English composure which Angelica Kauffmann has so skillfully represented on canvas. Seen in the various phases of his daily life, he gave the idea of being perfectly well-balanced, as exactly regulated as a Leroy chronometer. Phileas Fogg was, indeed, exactitude personified, and this was betrayed even in the expression of his very hands and feet; for in men, as well as in animals, the limbs themselves are expressive of the passions.

- GVKAFM EAR HKAIU AFCIKSAIT TACE OK. UDMM, XPRRIXPKCDVC EPG HIIF QPKIUVNNW DHRIKSAFM EAO. EI PXXIPKIG CD HI P OPF PHDVC UDKCW WIPKR DU PMI, TACE UAFI, EPFGRDOI UIPCVKIR, PFGP CPNN, TINN-REPXIG UAMVKI; EAR EPAK PFG TEARLIKR TIKI NAMEC, EAR UDKIEIPG QDOXPQC PFG VFTKAFLNIG, EAR UPQI KPCEIK XPNI, EAR CIICE OPMFAUAQIFC. EAR DVFCIFPFQI XDRRIRRIG AF CEIEAMEIRC GIMKII TEPC XEWRADMFDOARCR QPNN ‘KIXDRI AF PQCADF,’
- P JVPNACW DU CEDRI TED PQC KPCEIK CEPF CPNL. QPNO PFG XENIM-
- UKII IHDDLR PC XNPFIC IHDDL.QDO
- OPCAQ, TACE P QNIPK IWI, OK. UDMM RIIOIG P XIKUIQC CWXI DU CEPC IFMNARE QDOXDRVKI TEAQE PFMINAQP LPVUUOPFF EPR RDRLANUVNNW KIXKIRIFCIG DF QPFSPR. RIIF AF CEI SPKADVR XEPRIRDU EAR GPANW NAUI, EI MPSI CEI AGIP DU HIAFM XIKUIQCNW TINN-HPNPFQIG, PR IZPQCNW KIMVNPCIG PR P NIKDW QEKDFDOICIK. XEANIPRUDMM TPR, AFGIIG, IZPQCACVGI XIKRDFAUAIG, PFG CEAR TPR HICKPWIG ISIF AF CEI IZXKIRRADF DU EAR SIKW EPFGR PFG UIIC; UDK
- AF OIF, PR TINN PR AF PFAOPNR, CEI NAOHR CEIORINSIR PKI IZXKIRRASI DU CEI XPRRADFR.

EXAMPLE (CONTINUE)

- **Frequencies of letters in the text**

- E - 116,
- A - 78,
- S - 61,
- I - 57,
- T - 52,
- N - 49,
- H - 49,
- O - 43,
- R - 43,
- L - 37,
- F - 29,
- D - 27,
- C - 24,
- P - 23,
- G - 21,
- M - 19,
- W - 15,
- U - 15,
- Y - 14,
- B - 11,
- V - 9,
- K - 7,
- X - 4,
- Q - 1

- **Relative frequencies of letters in English language**

- e 0.12702
- t 0.09056
- a 0.08167
- o 0.07507
- i 0.06966
- n 0.06749
- s 0.06327
- h 0.06094
- r 0.05987
- d 0.04253
- l 0.04025
- c 0.02782
- u 0.02758
- m 0.02406
- w 0.02360
- f 0.02228
- g 0.02015
- y 0.01974
- p 0.01929
- b 0.01492
- v 0.00978
- k 0.00772
- j 0.00153
- x 0.00150
- q 0.00095
- z 0.00074

OTHER CLASSICAL CIPHERS

- *Vigenère cipher*
- First described by Giovan Battista Bellaso
- in 1553.

- *Playfair cipher*
- It was invented by Charles Wheatstone,
- who first described it in 1854.

- *Vernam cipher*
- Named after Gilbert Sandford Vernam
- who invented it in 1917.

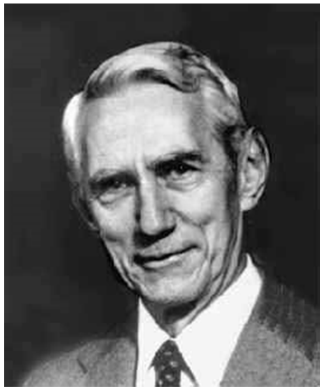
SECOND PERIOD - WWII

A. Turing

(23/6/1912 –7/6/ 1954)

Team (hut) 8, Bletchley Park

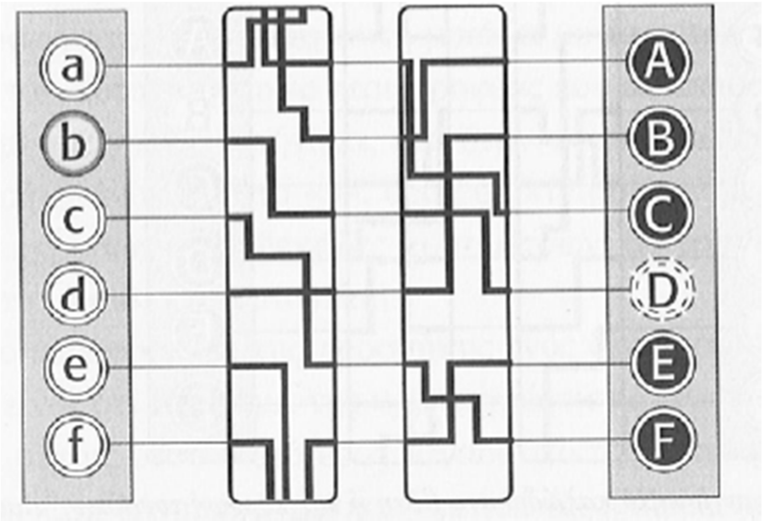
(1949):«Communication Theory of Secrecy Systems», Bell System Technical Journal, vol.28(4), page 656–715, 1949.

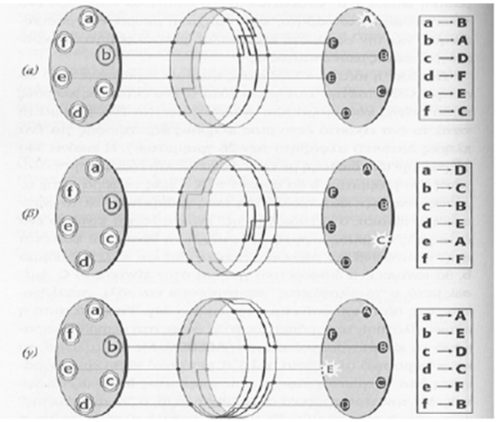


C. Shannon

(30/4/1916 –24/2/ 2001)

ENIGMA





Assistant Professor, Harokopio University of Athens, Greece

THIRD PERIOD

- The new era

- Well studied algorithms and protocols
- Academia (Bsc courses, Msc programs, research)
- Commercial applications
- Standardization bodies
- Certification
- Several billions market
- Cyberwars and allinces

THIRD PERIOD

- 1976: «New Directions in Cryptography», in
- IEEE Transactions on information theory by
- Bailey Whitfield Diffie and Martin Hellman

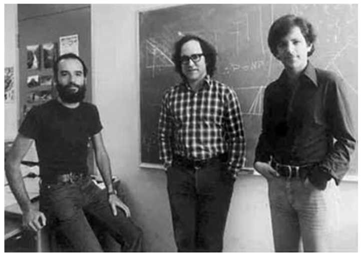
- 1977: Data Encryption Standard (DES) becomes
- official Federal Information Processing Standard (FIPS)
- for the United States

- 1978: RSA algorithm (Rivest – Shamir – Adleman)

- January 14, 2000: U.S. Government announce restrictions on
- export of cryptography are relaxed

- 2001: Rijndael algorithm selected as the U.S. Advanced Encryption
- Standard (AES) after a five-year public search process by
- National Institute for Standards and Technology (NIST)

Bailey Whitfield Diffie
Martin Hellman

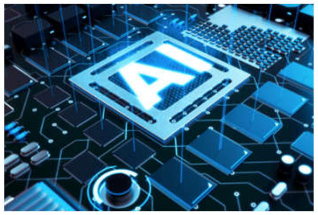


CHALLENGES AND OPEN PROBLEMS

1. Lightweight cryptography for IoT

2. Big data cryptography

3. AI cryptography



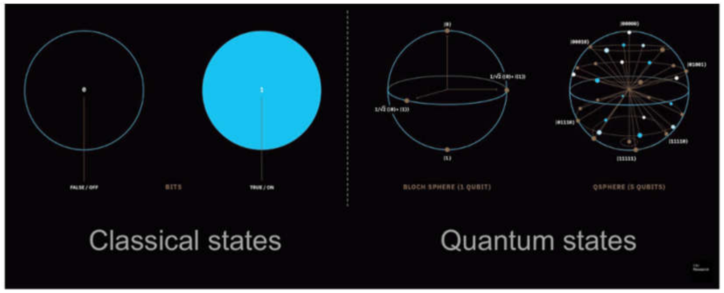
4. Post Quantum Cryptography

FOURTH PERIOD

- 1981 - Richard Feynman proposed
- quantum computers.

- Most of the cryptographically interesting hard mathematical problems can be solved efficiently.

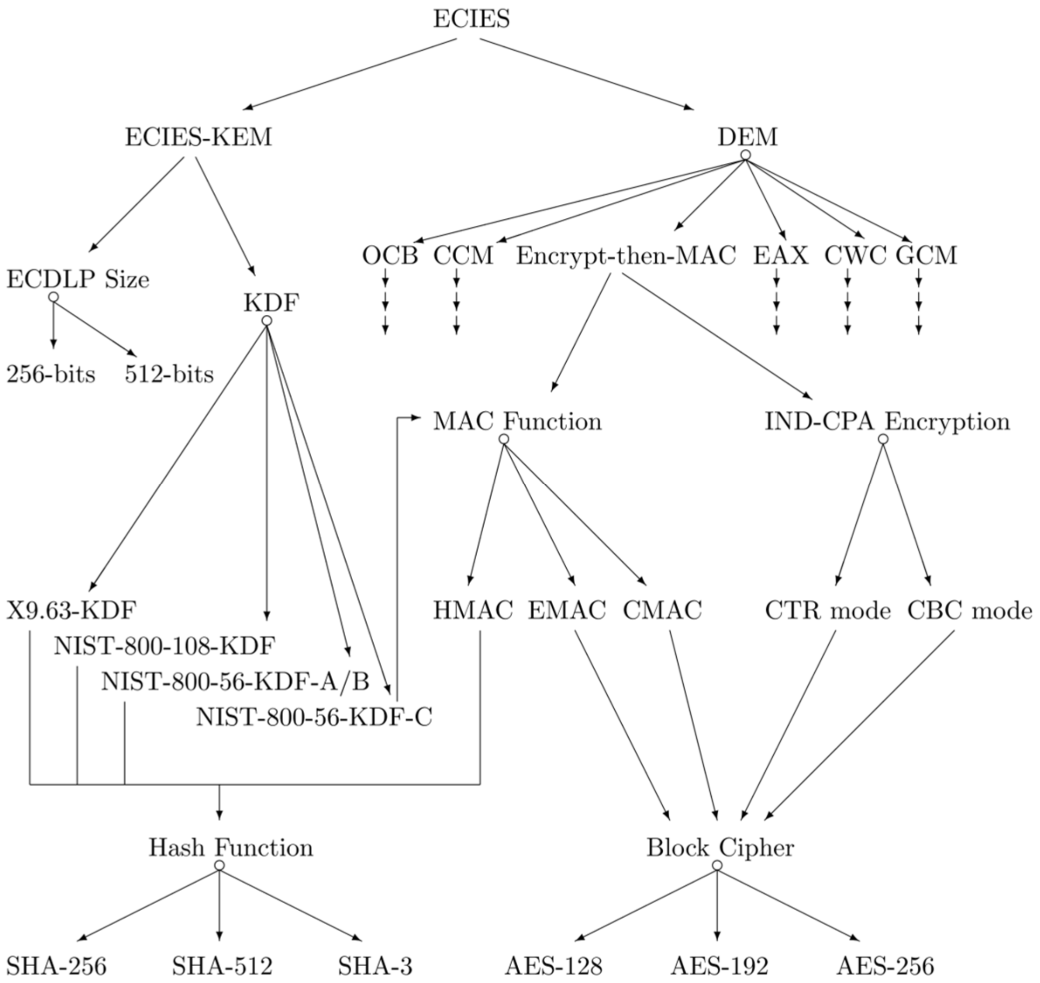
- PQ standardization competition by NIST
- https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization



CRYPTO AGENDA

Assistant Professor, Harokopio University of Athens, Greece

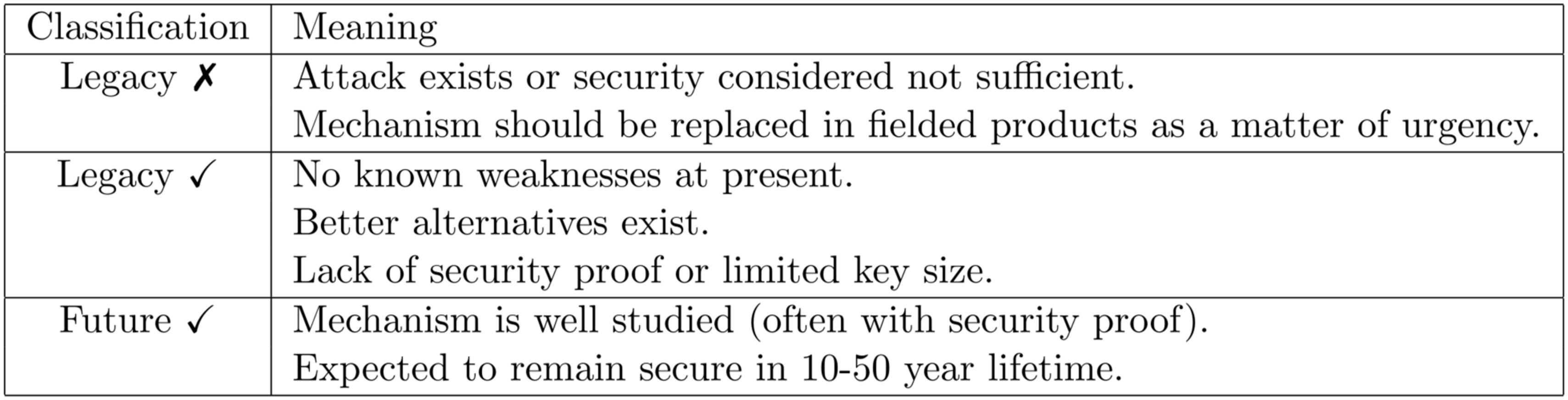
OVERVIEW



*** Algorithms, key size and parameters report. ENISA– 2014**

Assistant Professor, Harokopio University of Athens, Greece

CLASSIFICATION



Classification	Meaning
Legacy ✗	Attack exists or security considered not sufficient. Mechanism should be replaced in fielded products as a matter of urgency.
Legacy ✓	No known weaknesses at present. Better alternatives exist. Lack of security proof or limited key size.
Future ✓	Mechanism is well studied (often with security proof). Expected to remain secure in 10-50 year lifetime.

SOME REFERENCES

- Everyday Cryptography: Fundamental Principles and Applications, Keith M. Martin, oxford press
- The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Simon Singh
- New directions in Cryptography
- https://ee.stanford.edu/~hellman/publications/24.pdf
- ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012)
- ENISA, Algorithms, key size and parameters, report – 2014
- ECRYPT – CSA, Algorithms, Key Size and Protocols Report (2018)

SOME REFERENCES

- Lecture Notes on Cryptography, Shafi Goldwasser, 1 Mihir Bellare (check the reading material folder)
- Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone (too old, but free) http://cacr.uwaterloo.ca/hac/
- Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell (2nd Edition!)
- http://www.cs.umd.edu/~jkatz/imc.html
- Papers
- Other books

Assistant Professor, Harokopio University of
Athens, Greece