Cryptography
Lecture 1

Dr. Panagiotis Rizomiliotis

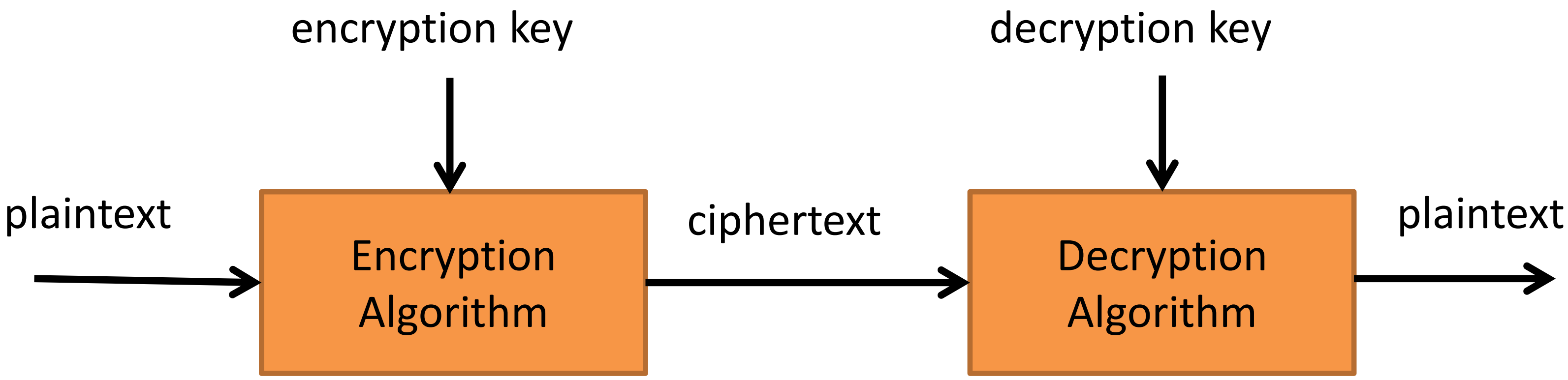
Agenda

- Introduction
- History of cryptography
- Crypto agenda

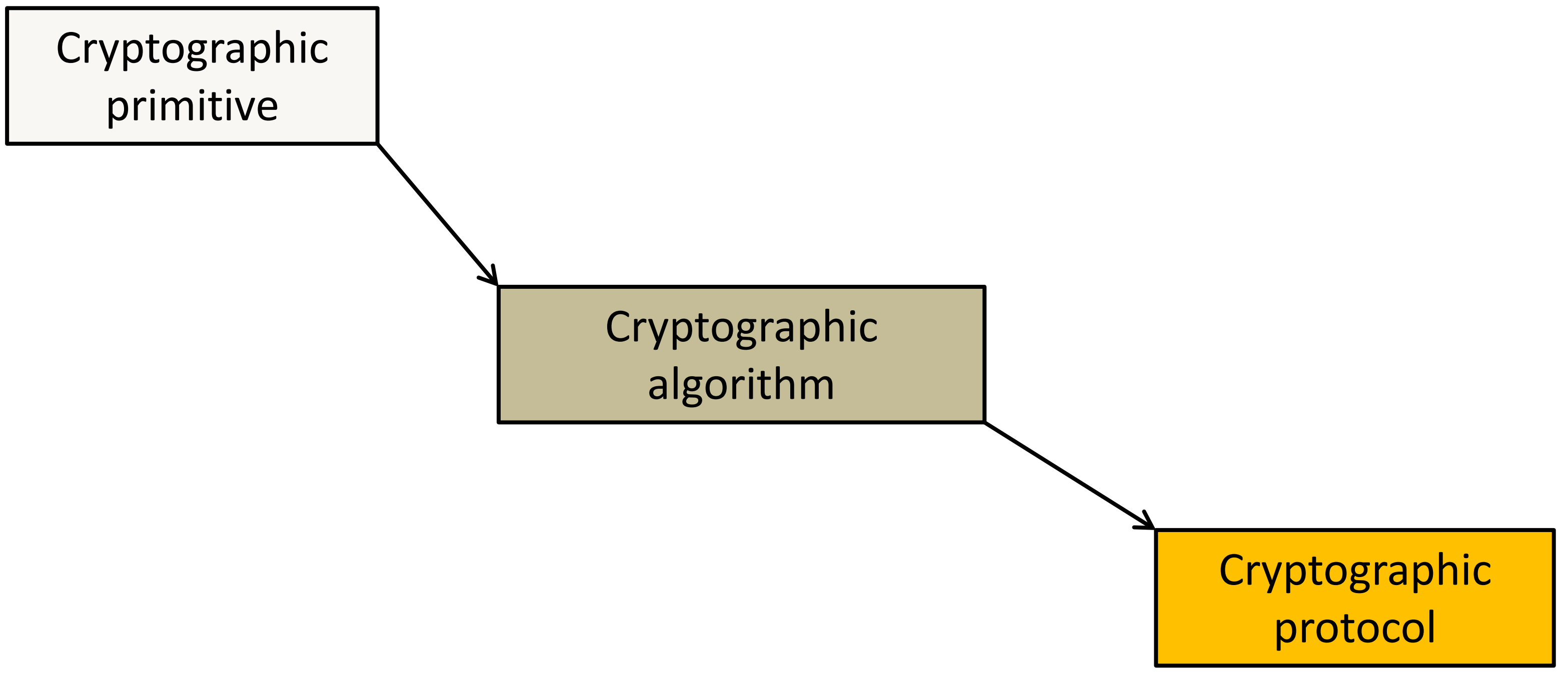
definitions

- Cryptography
- Cryptanalysis
- Cryptology
- Cryptosystem

Basic model of a cryptosystem



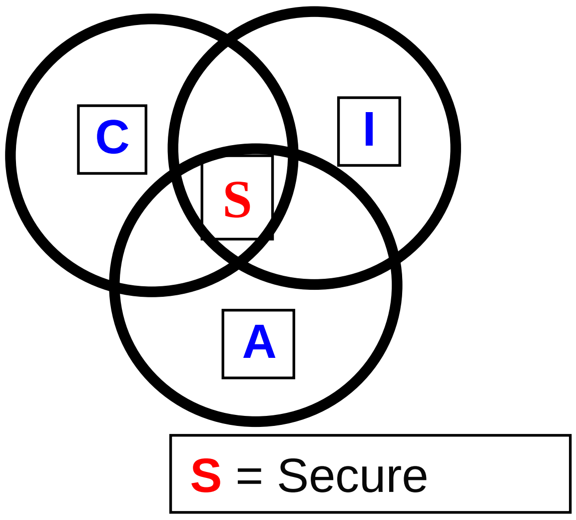
(more) definitions



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

Hi!!! I am Alice

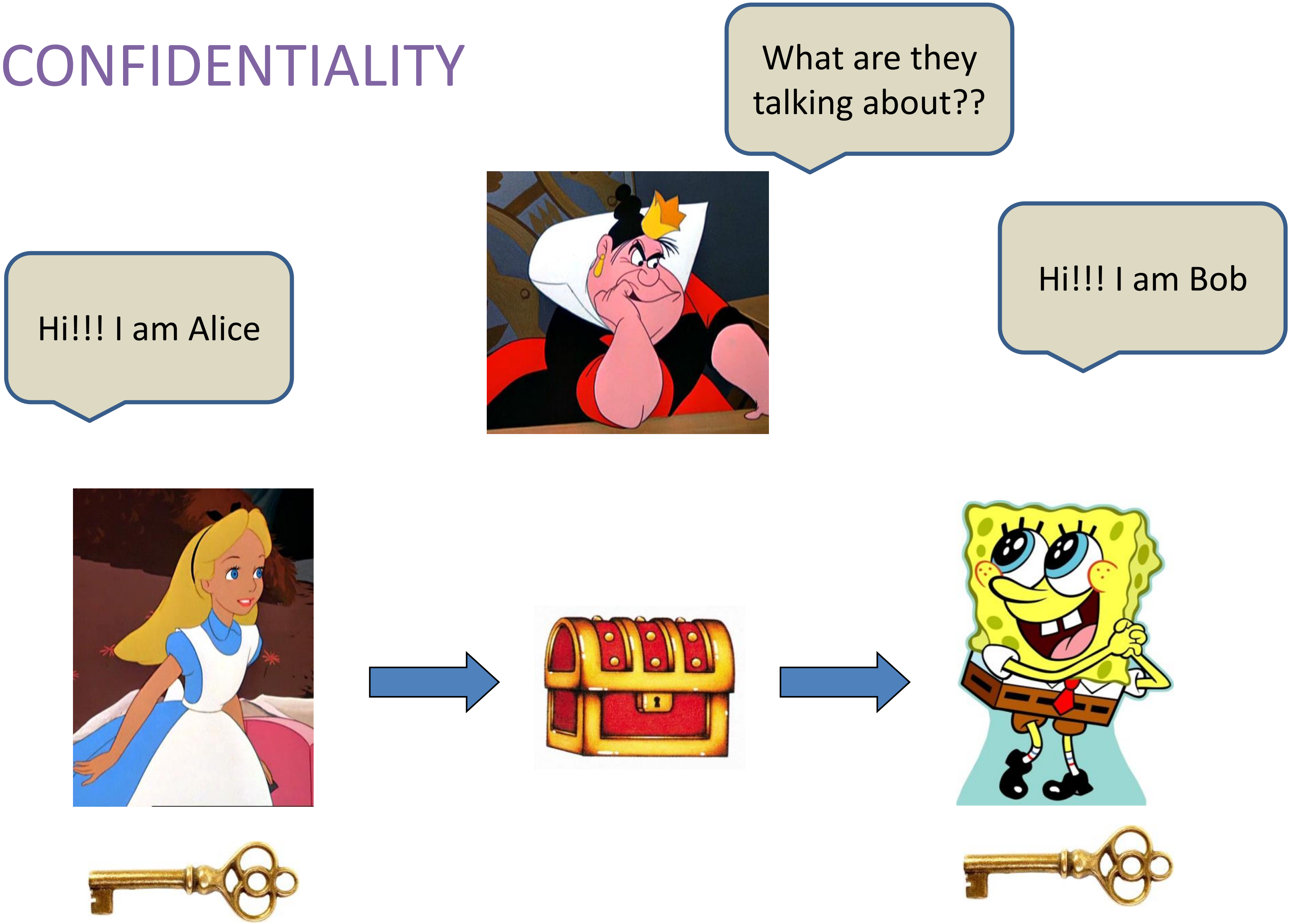
And I am Eve

Hi!!! I am Bob

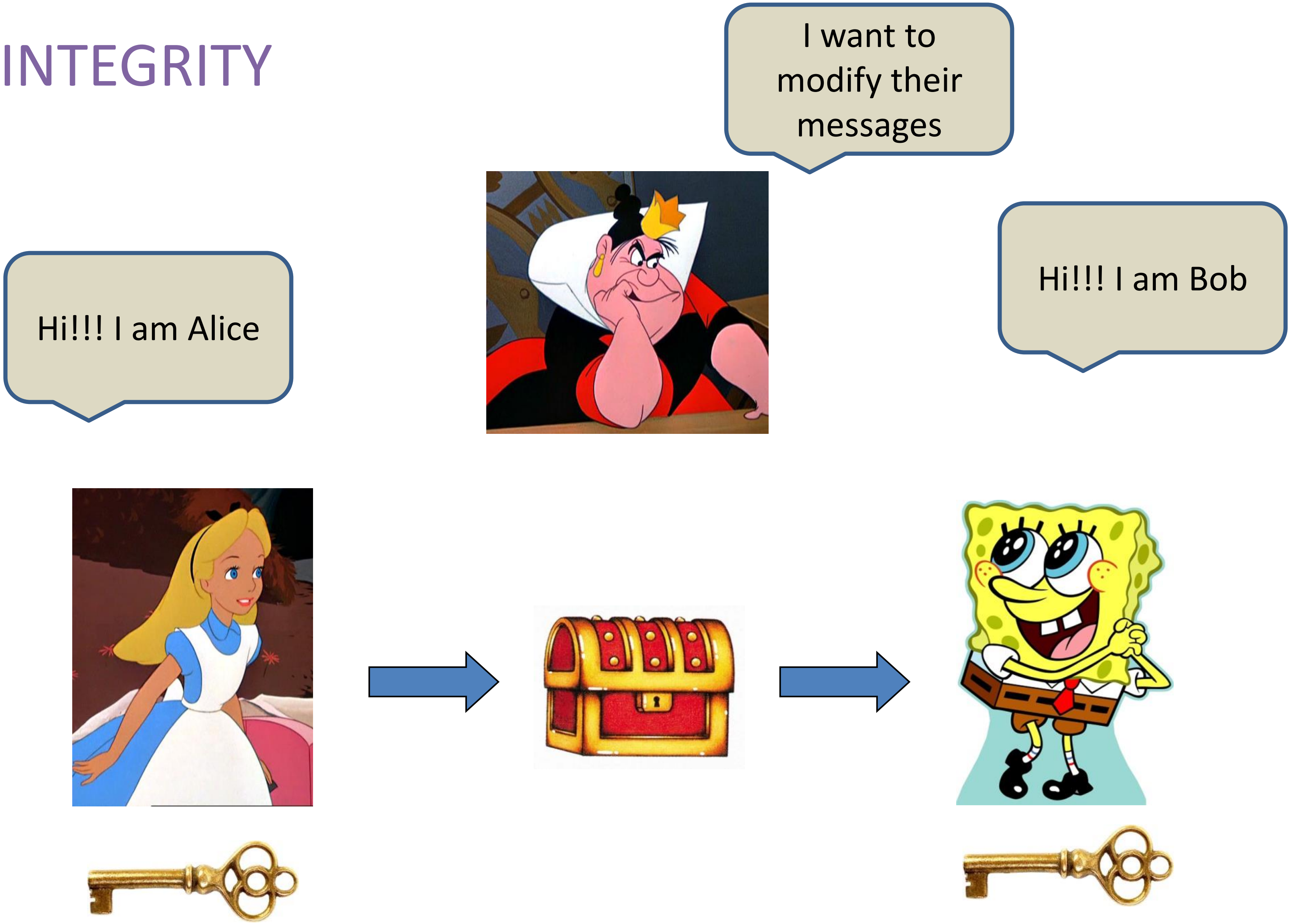
Insecure Channel

This is an attack model…

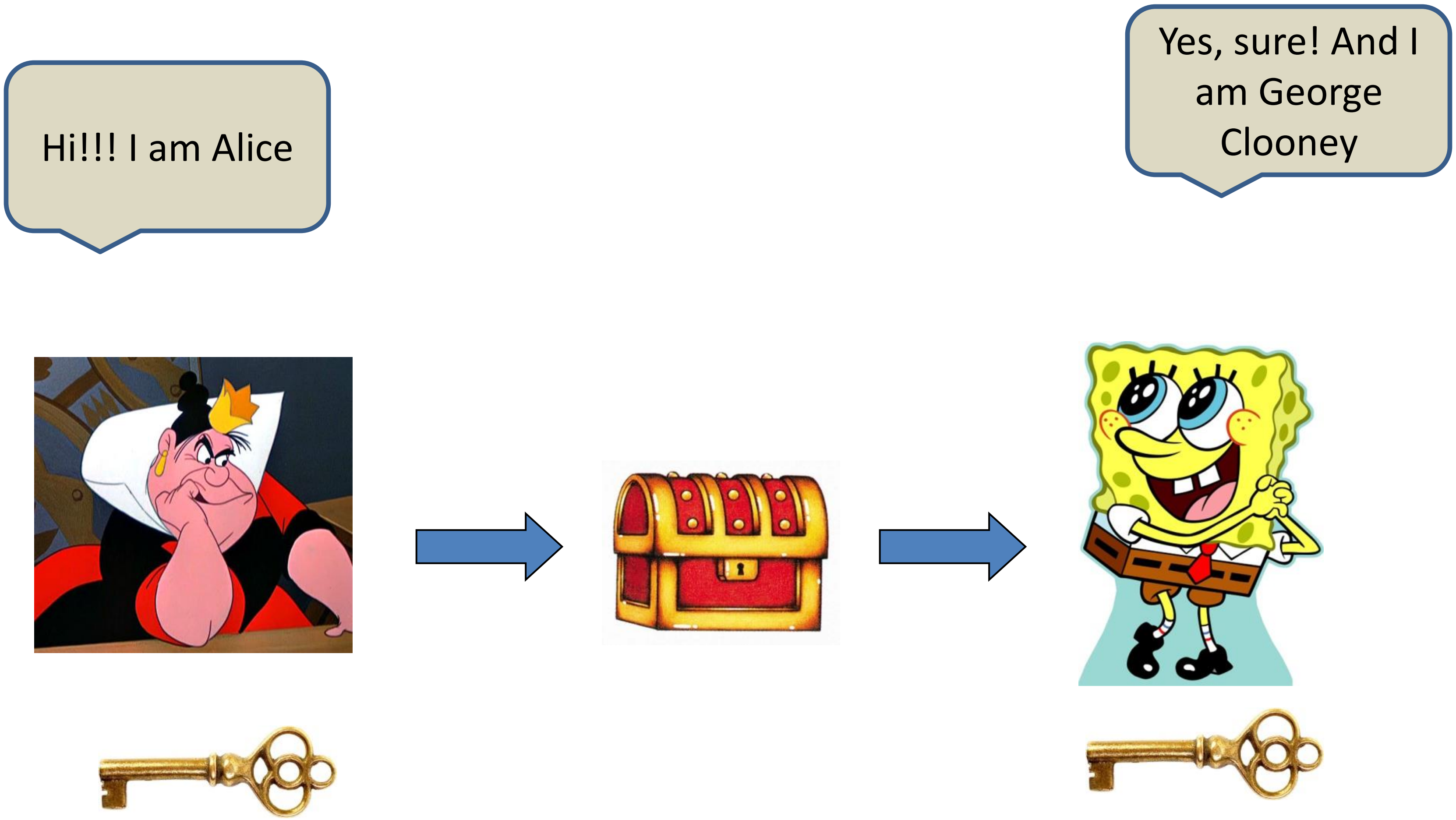
CONFIDENTIALITY



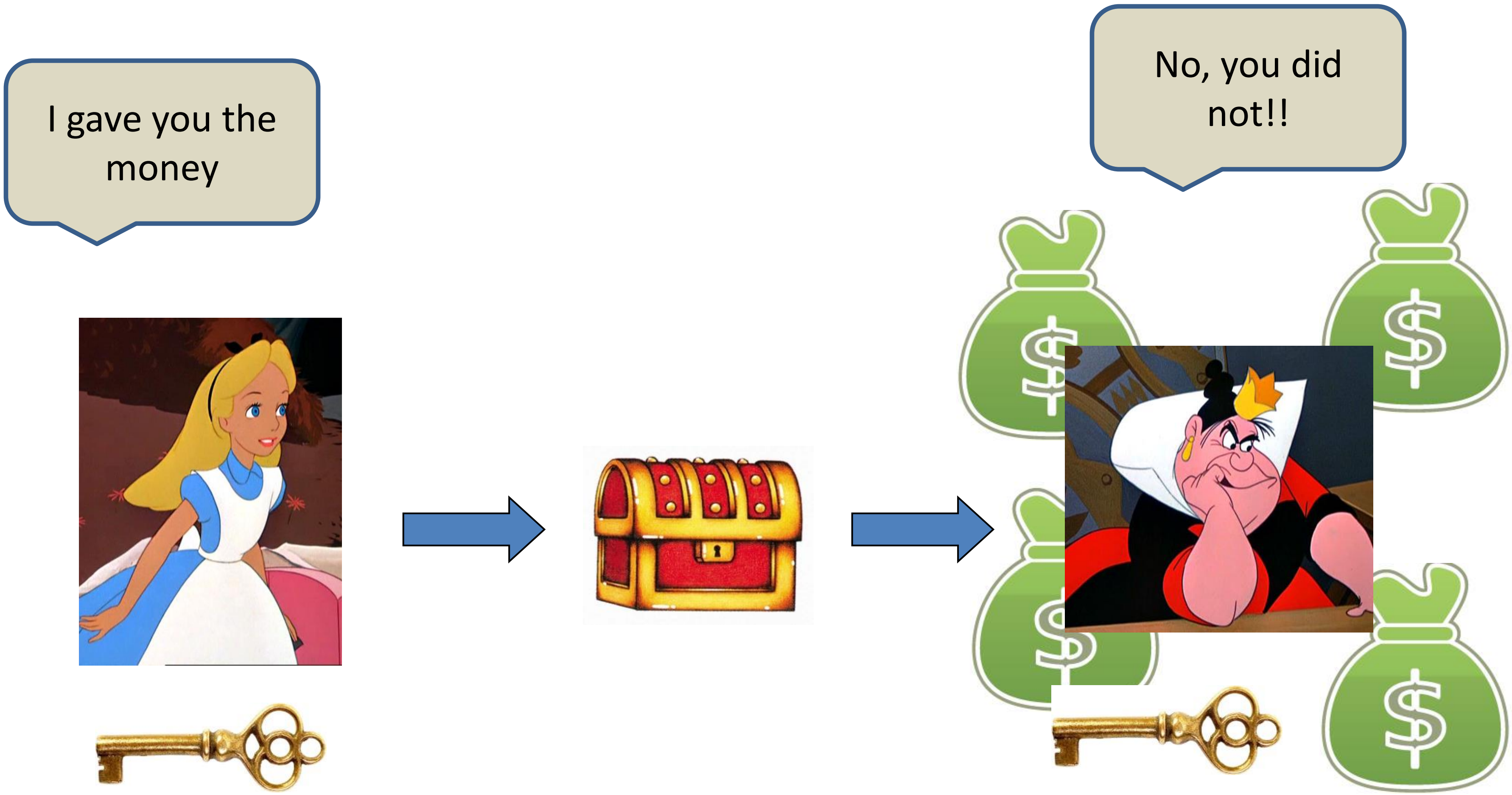
INTEGRITY



AUTHENTICATION



NON – REPUDIATION

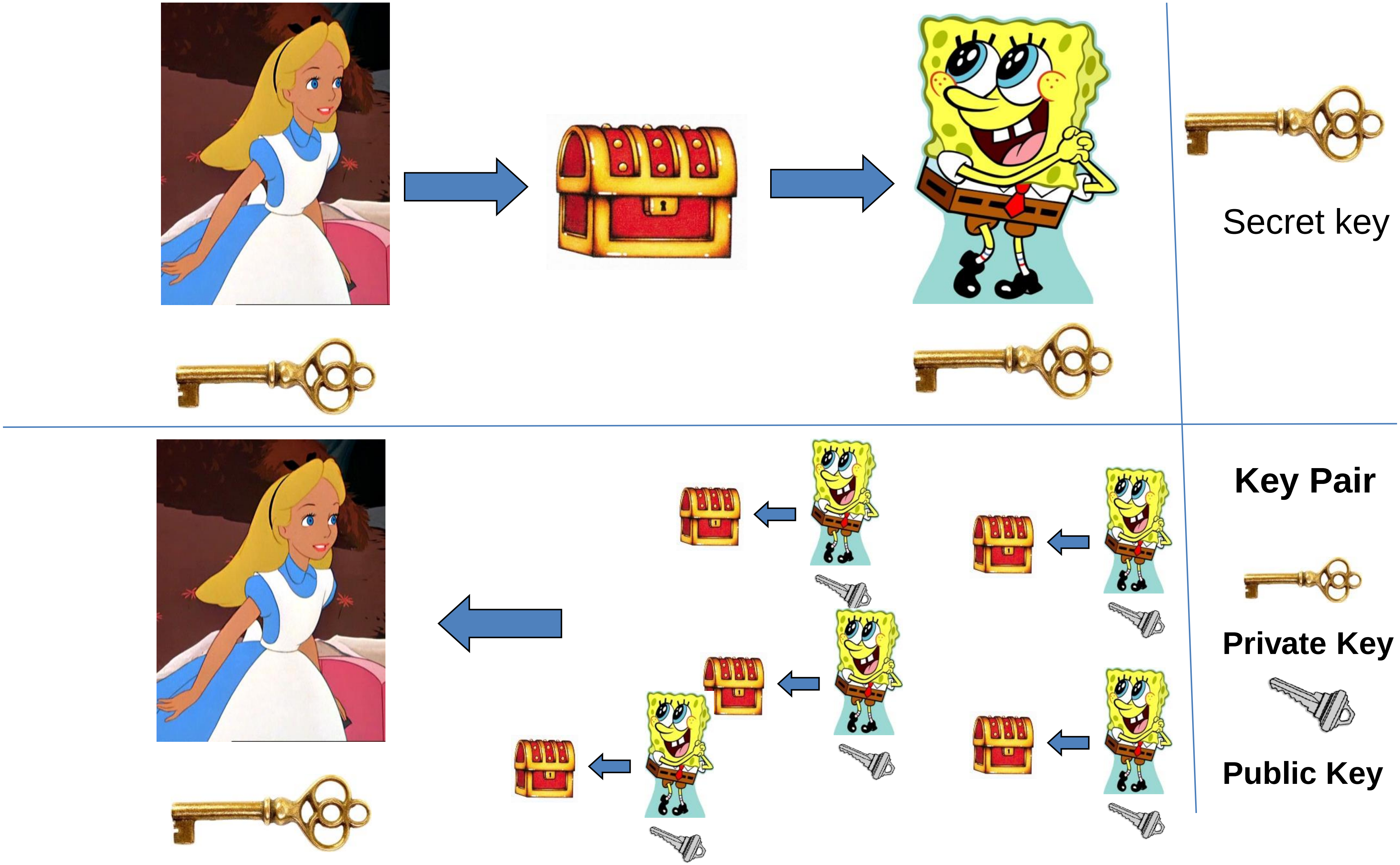


TYPES OF CRYPTOSYSTEMS

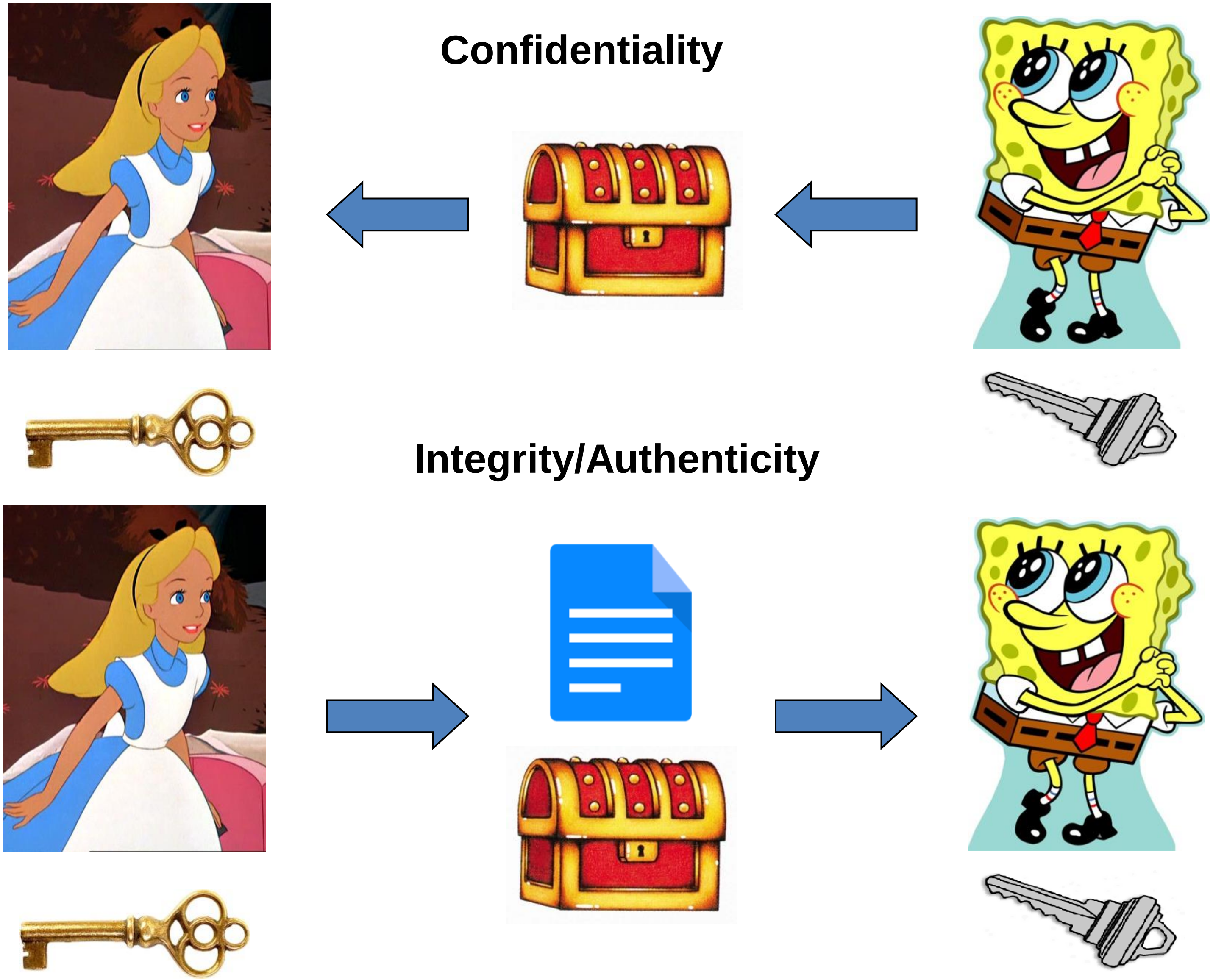
- **Two types of cryptosystems**

1. Symmetric key
2. Asymmetric or public key

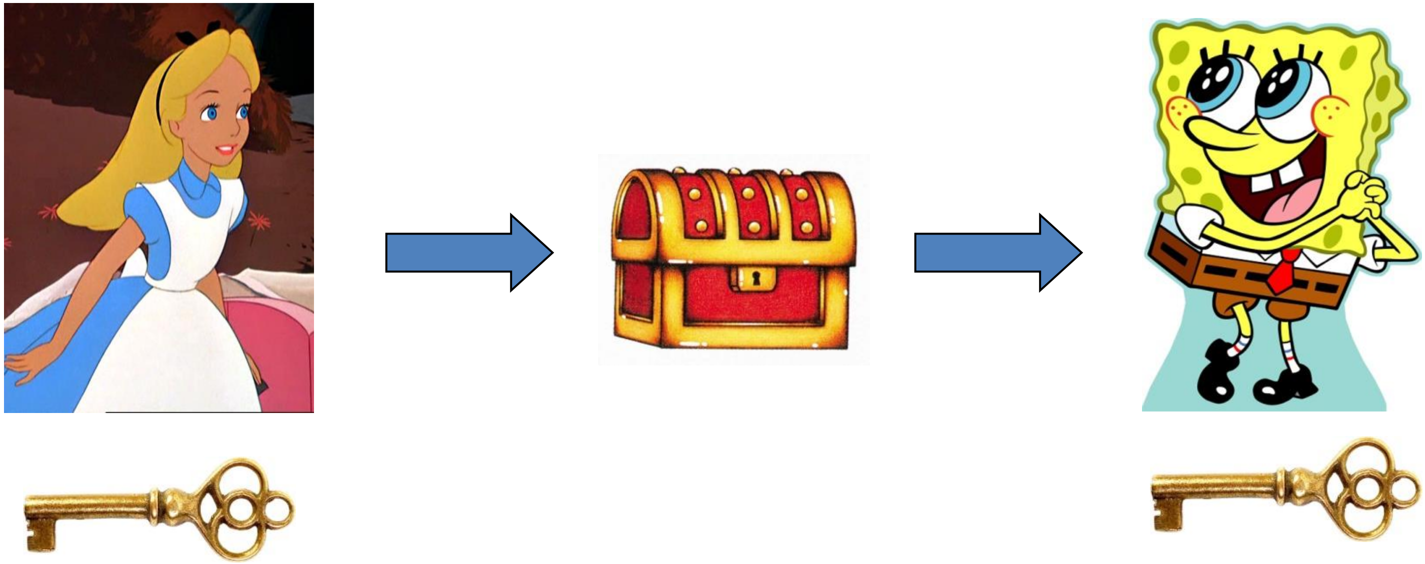
SYMMETRIC KEY VS PUBLIC KEY



ASYMMETRIC KEY (PUBLIC KEY)



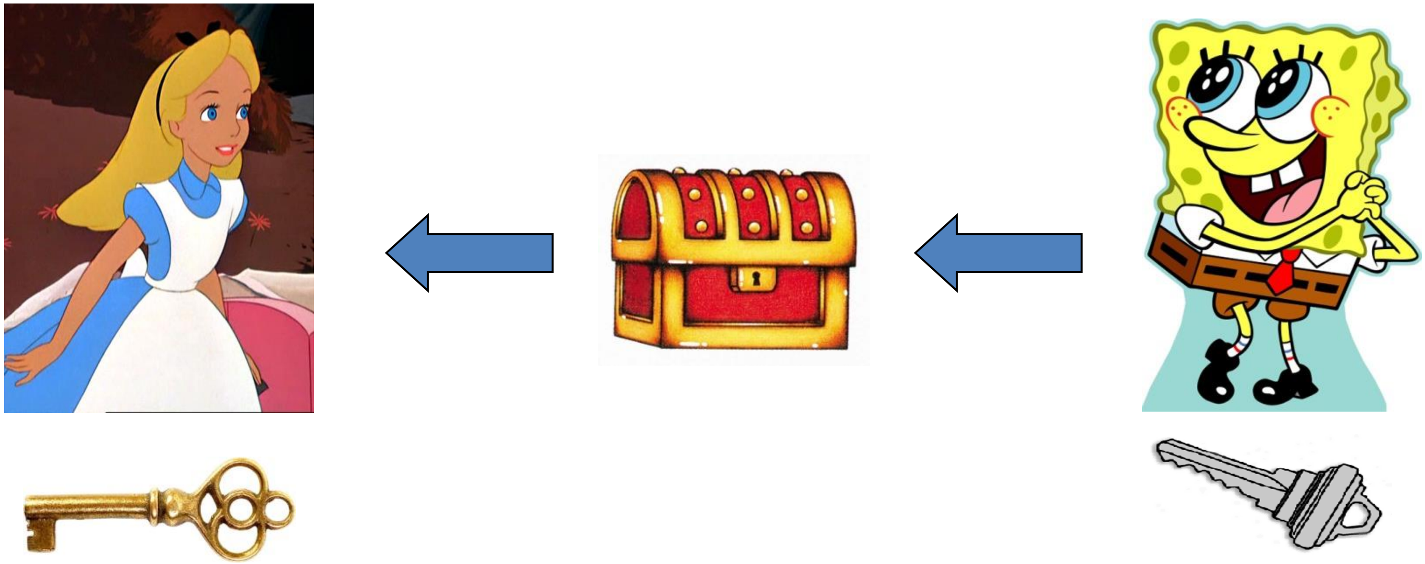
SYMMETRIC KEY – KEY EXCHANGE

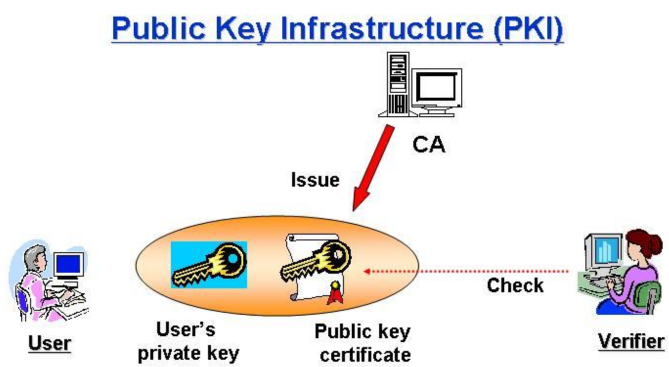


Trusted Third Party (TTP)

Meeting place

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!!!

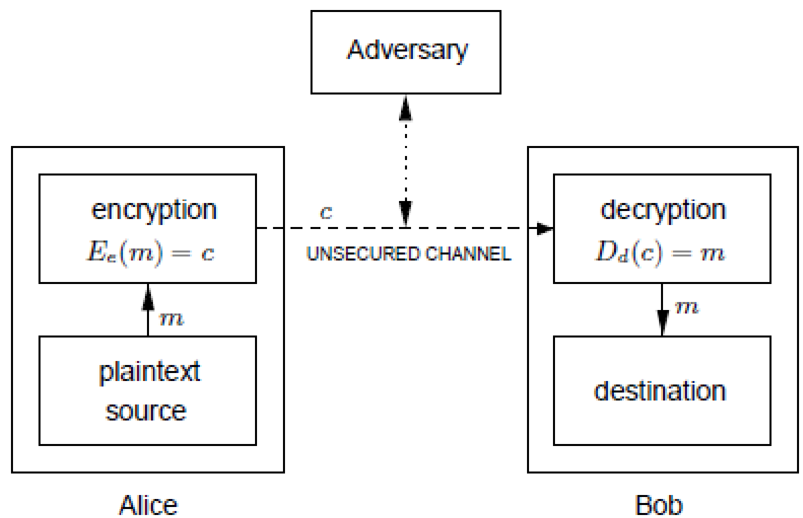
Adversary model

- Passive
  - Usually an eavesdropper
  - Honest but curious

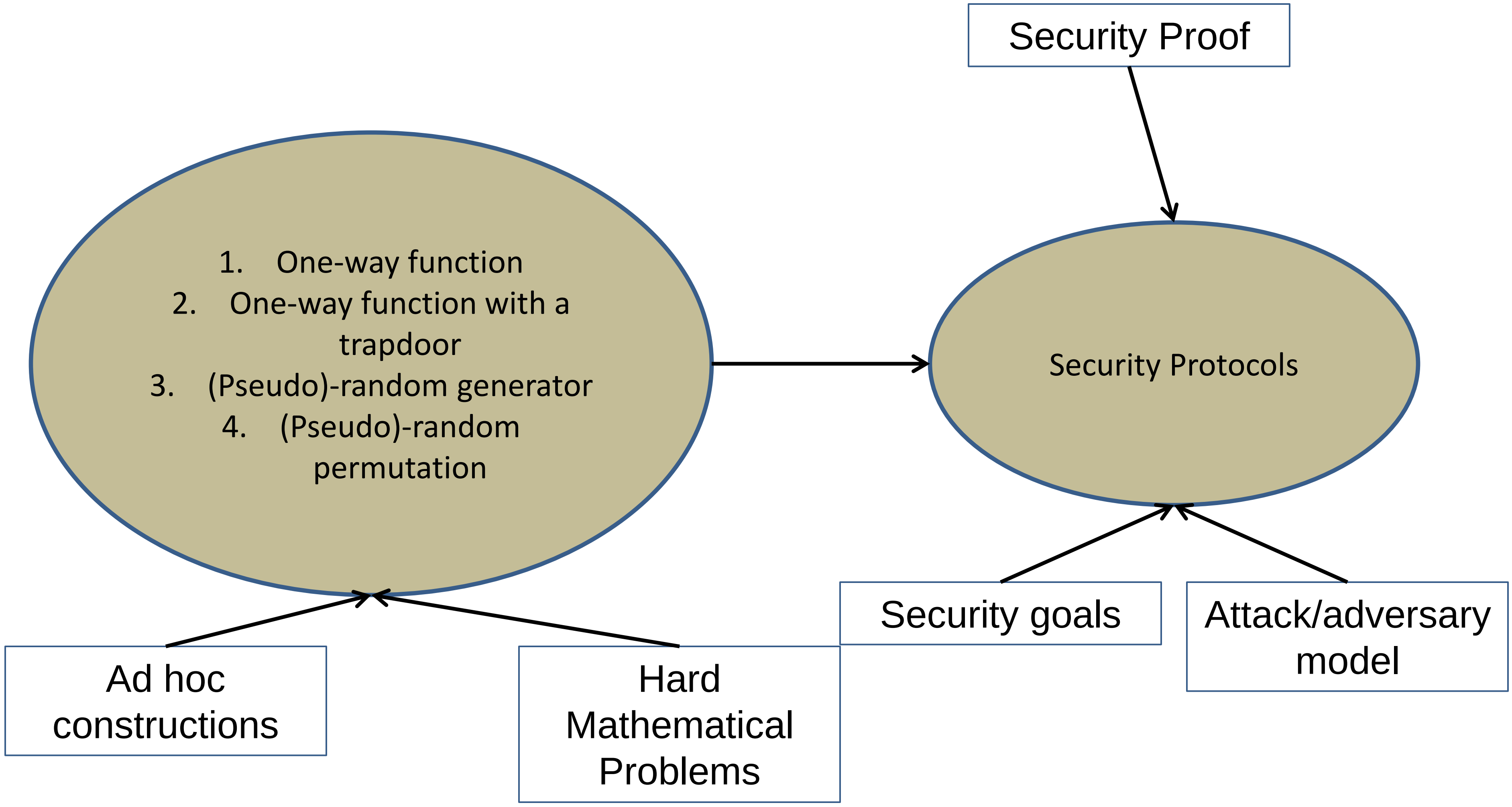
- Active
  - She can modify the messages
- more powerful adversary
- can request a polynomial number of ciphertexts to be decrypted for him
- intercept messages being transmitted from sender to receiver and either stop their delivery all together or alter them in some way

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-cip



BASIC STEPS



Security Proof
1. One-way function
2. One-way function with a trapdoor
3. (Pseudo)-random generator
4. (Pseudo)-random permutation
Security Protocols
Security goals
Attack/adversary model
Ad hoc constructions
Hard Mathematical Problems

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, 3.31×10^{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

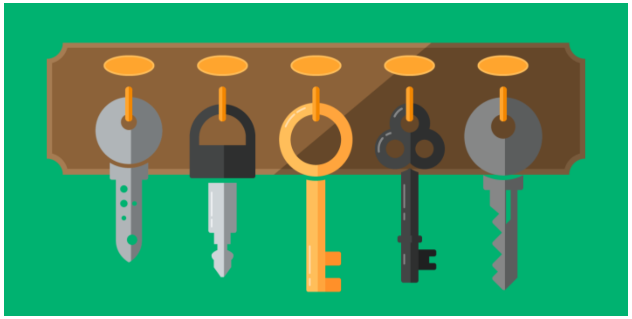
- Theoretical (or academic) attacks
- An attack that it is more efficient than the alleged bound, but still far from practical

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…

CRYPTOGRAPHIC HISTORY

A very old story…

- We can identify the 4 main historical periods:

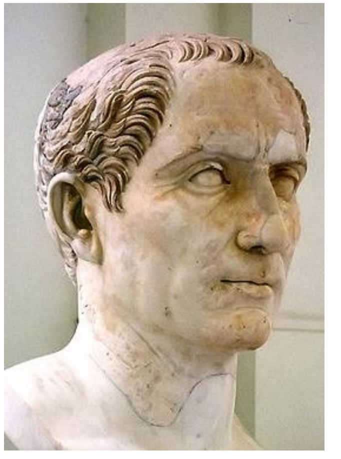
1. 4000 BC until WW II
2. WW II until the 70s
3. The 70s until today
4. The Quantum Computing Era

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

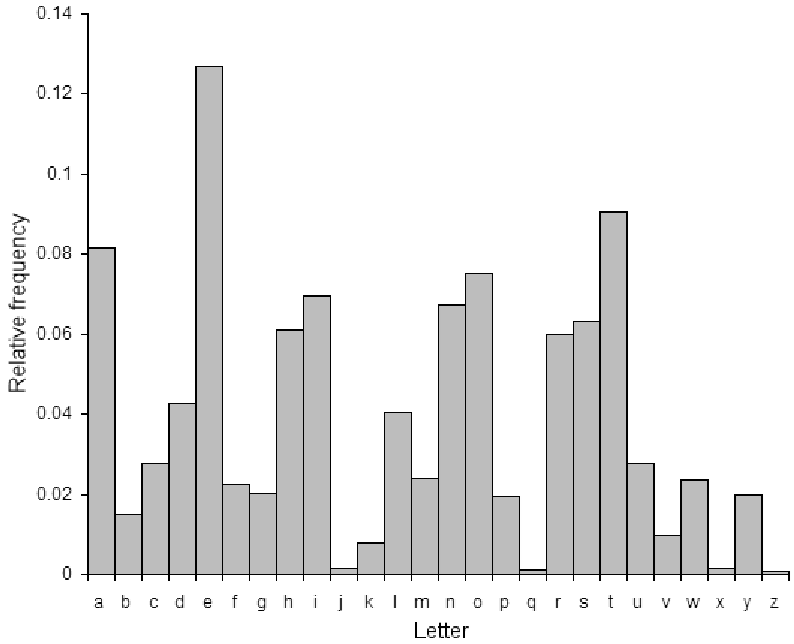
- Secret key: The size of keyspace is 26! (factorial) = $4x10^{26}$
- n!=n x (n-1) x …x 1

- *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

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

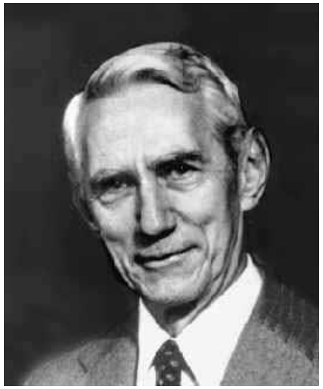
- Enigma

A. Turing

(23/6/1912 –7/6/ 1954)

Team (hut) 8, Bletchley Park

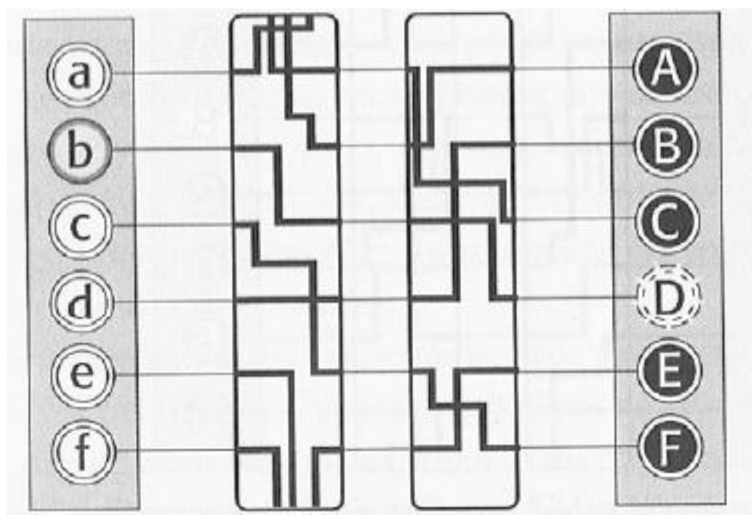
(1949):«Communication Theory of Secrecy Systems», Bell System Technical Journal, vol.28(4), page 656–715, 1949.

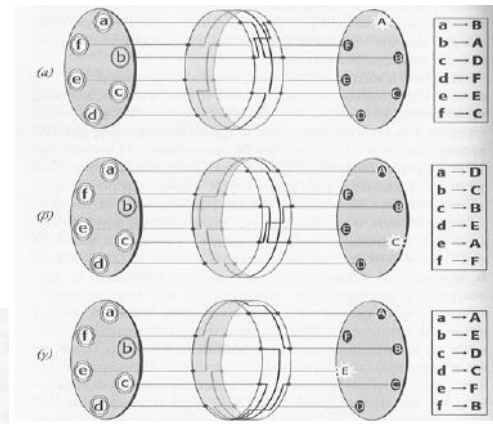


C. Shannon

(30/4/1916 –24/2/ 2001)

Enigma





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

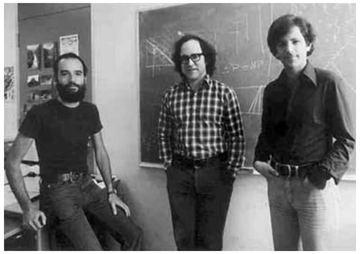
- 1977: Data Encryption Standard (DES) becomes
- official Federal Information Processing Standard (FIPS)
- for the United States

- 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

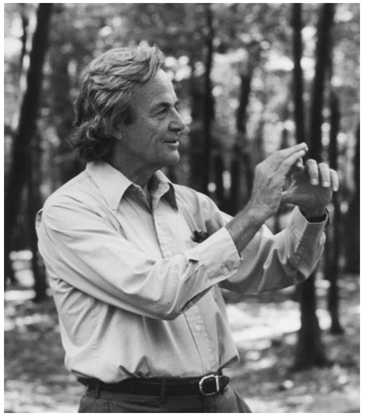
1. Lightweight cryptography for IoT

2. Big data cryptography

3. AI cryptography

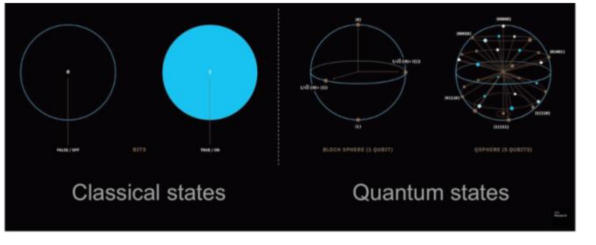
4. Post Quantum Cryptography

Fourth period



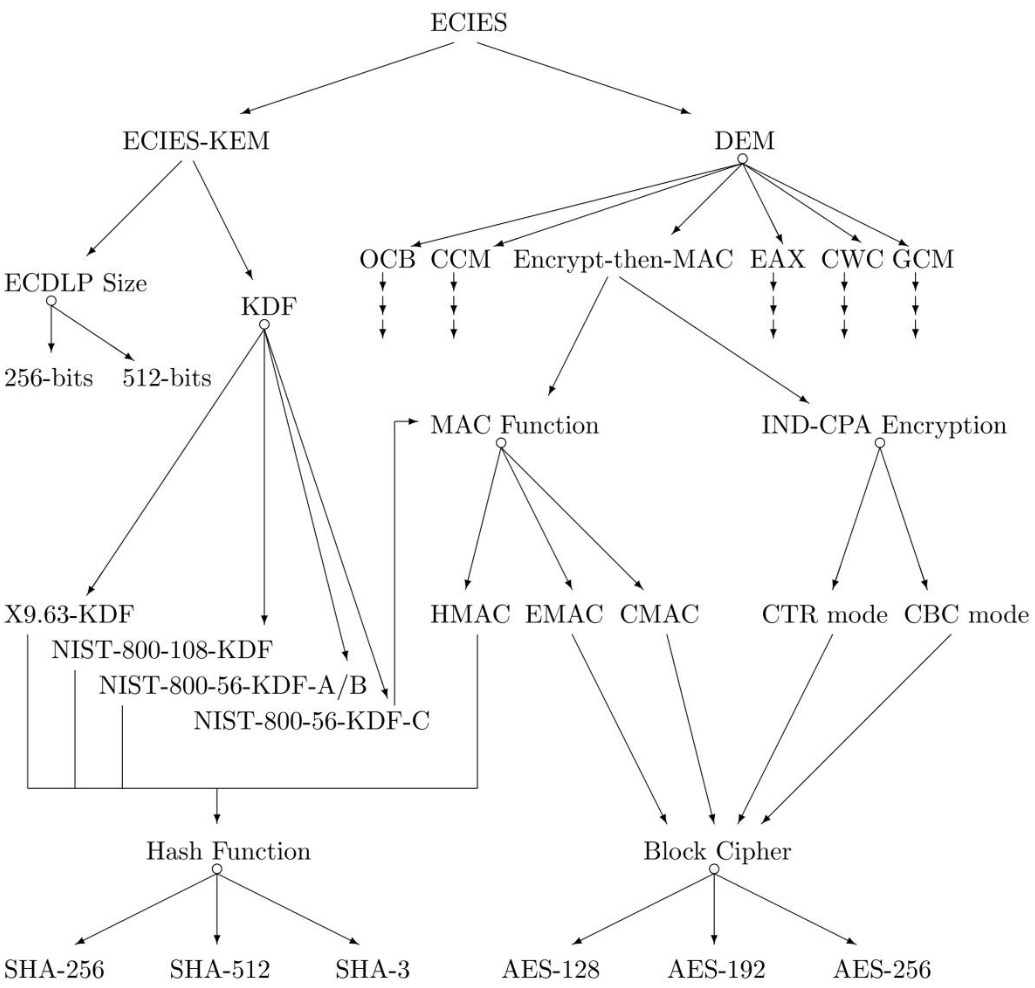
- 1981 - Richard Feynman proposed
- quantum computers.

- 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

Overview



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

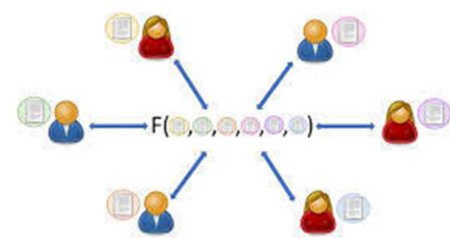
Classification

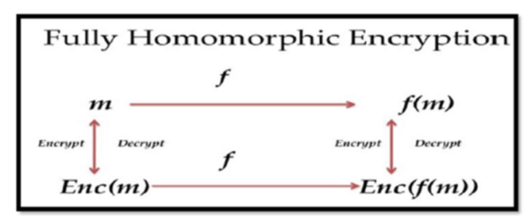
Classification	Meaning
Legacy ✗	Attack exists or security considered not sufficient. Mechanism should be replaced in fielded products as a matter of urgency.
Legacy ✓	No known weaknesses at present. Better alternatives exist. Lack of security proof or limited key size.
Future ✓	Mechanism is well studied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

In galaxy (not) so far away

- "Traditional" Cryptography is dealing with
  - P2P security (secure channel)
  - Storage
  - Authentication of data

- We are rapidly moving to the advance Crypto era (confidential computation)
  - Multiparty Computation
  - (Fully) Homomorphic Encryption
  - Zero knowledge proofs (ZK-SNARKs)





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)

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!)
- Cryptography Made Simple. Nigel Smart. Springer
- http://www.cs.umd.edu/~jkatz/imc.html
- Papers
- Other books


Questions?