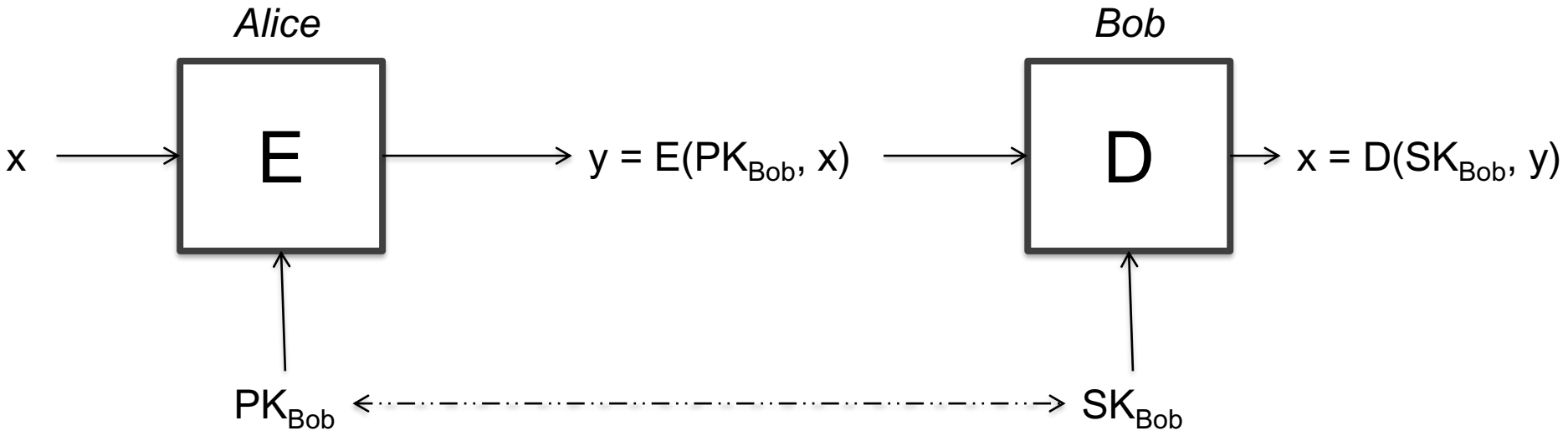
Public Key Cryptography

Gianluca Dini
Dept. Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@unipi.it
Version: 2021-03-29

Public Key Cryptography

INTRODUCTION

Public key encryption



- $pubK_{Bob}$: public key
- $privK_{Bob}$: private key

OGNI UTENTE HA 2 CHIAVI

- Alice knows Bob's public key $pubK_{Bob}$
- Bob keeps secret his own private key $privK_{Bob}$

FOCUS SU CONFIDENZIALITÀ!

Public key encryption - Definition

- A public key encryption scheme is a triple of algs (G, E, D) s.t.
  - G is a randomized alg. for key generation (pk, sk)
  - y = E(pk, x) is a randomized alg. that takes x ∈ M and outputs y ∈ C
  - x = D(sk, y) is deterministic alg. that takes y ∈ C and outputs x ∈ M
  - fulfill the consistency property
    - ∀(pk, sk), ∀ x ∈ M, D(sk, E(pk, x)) = x

Security of PKE: informal

- Known pk ∈ K and y ∈ C, it is computationally infeasible to find the message x ∈ M such that E(pk, x) = y
- Known the public key pk ∈ K, it is computationally infeasible to determine the corresponding secret key sk ∈ K
- Constructions generally rely on hard problems from number theory and algebra

PKE is not perfect

UNIVERSITÀ DI PISA

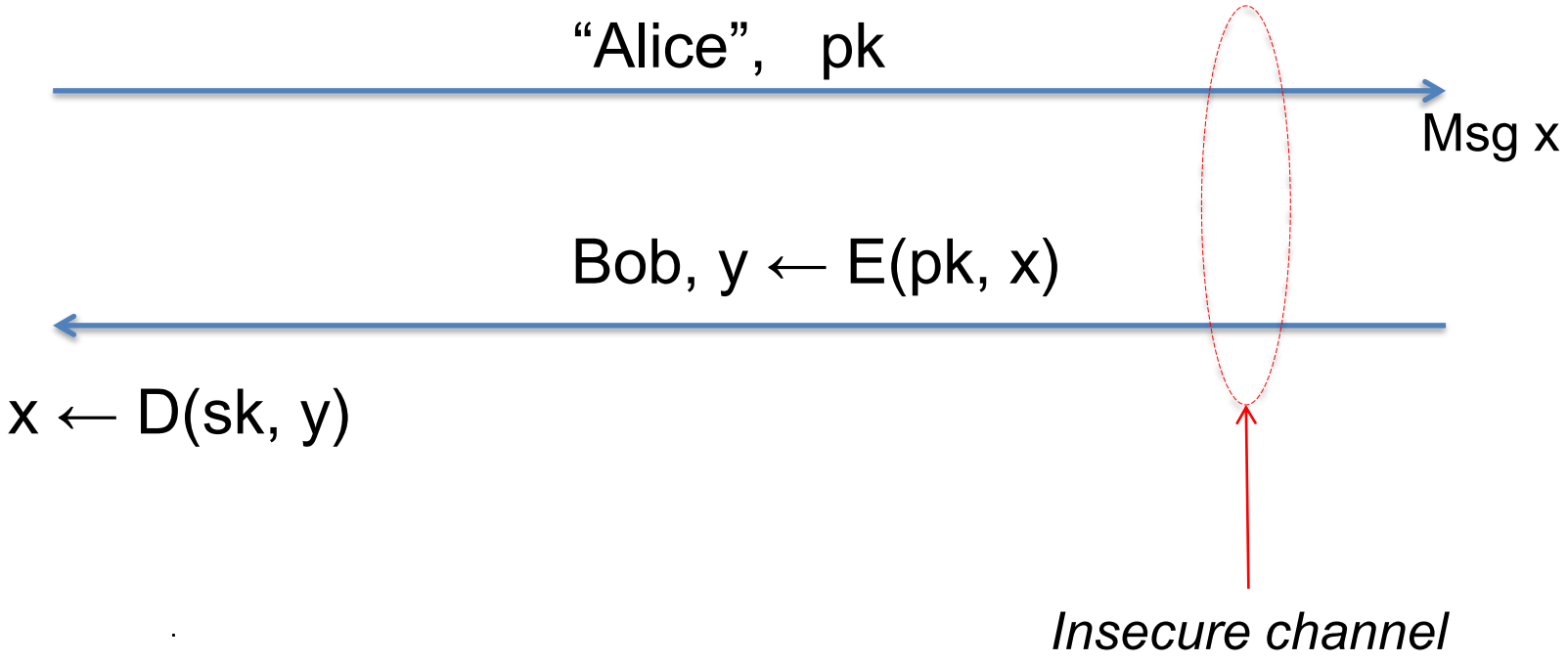
- PK encryption scheme is not perfect
  - Proof
    - Let y = E(pk, x)
    - Adversary intercepts y over the channel
    - Adversary
      - selects x' s.t. Pr[M = x'] ≠ 0 (a priori)
      - computes y' = E(pk, x')
      - If y' == y (a posteriori)
        then x' = x and Pr[M = x' | C = y] = 1
        else Pr[M = x' | C = c] = 0

PKE basic protocol

UNIVERSITÀ DI PISA

Alice **Bob**

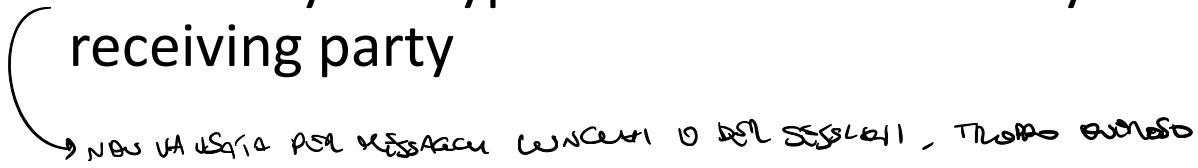
(pk, sk) ⟵ G()



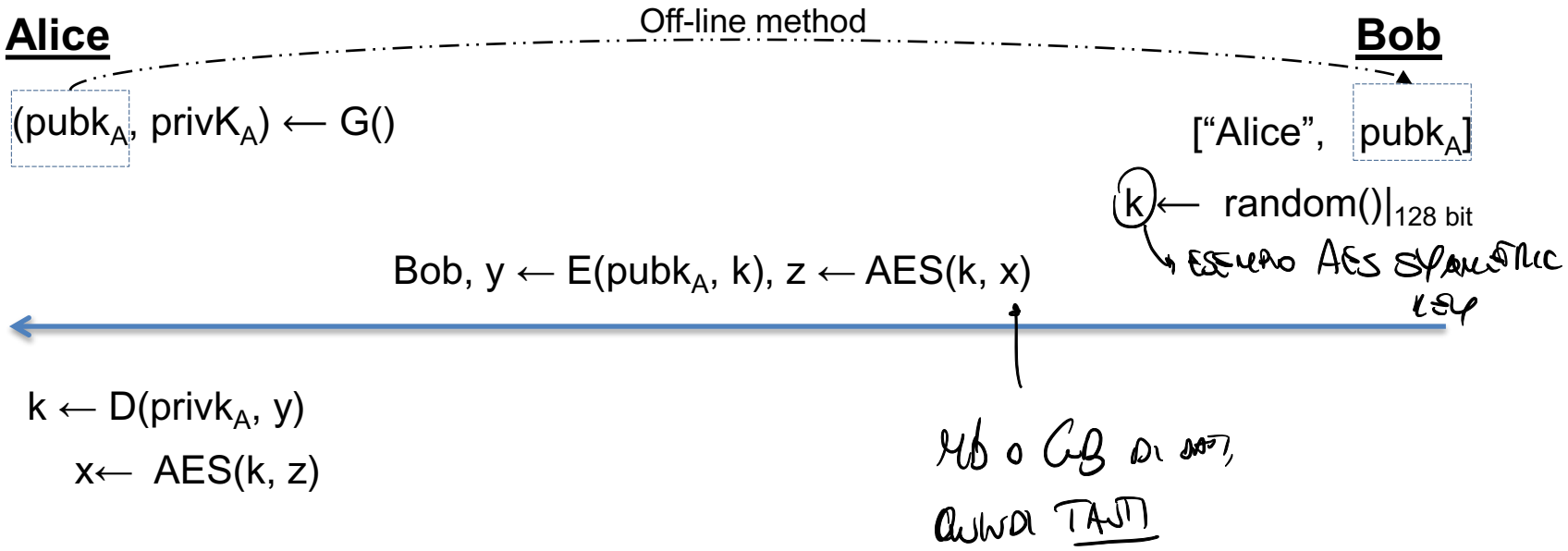
Digital envelope

UNIVERSITÀ DI PISA

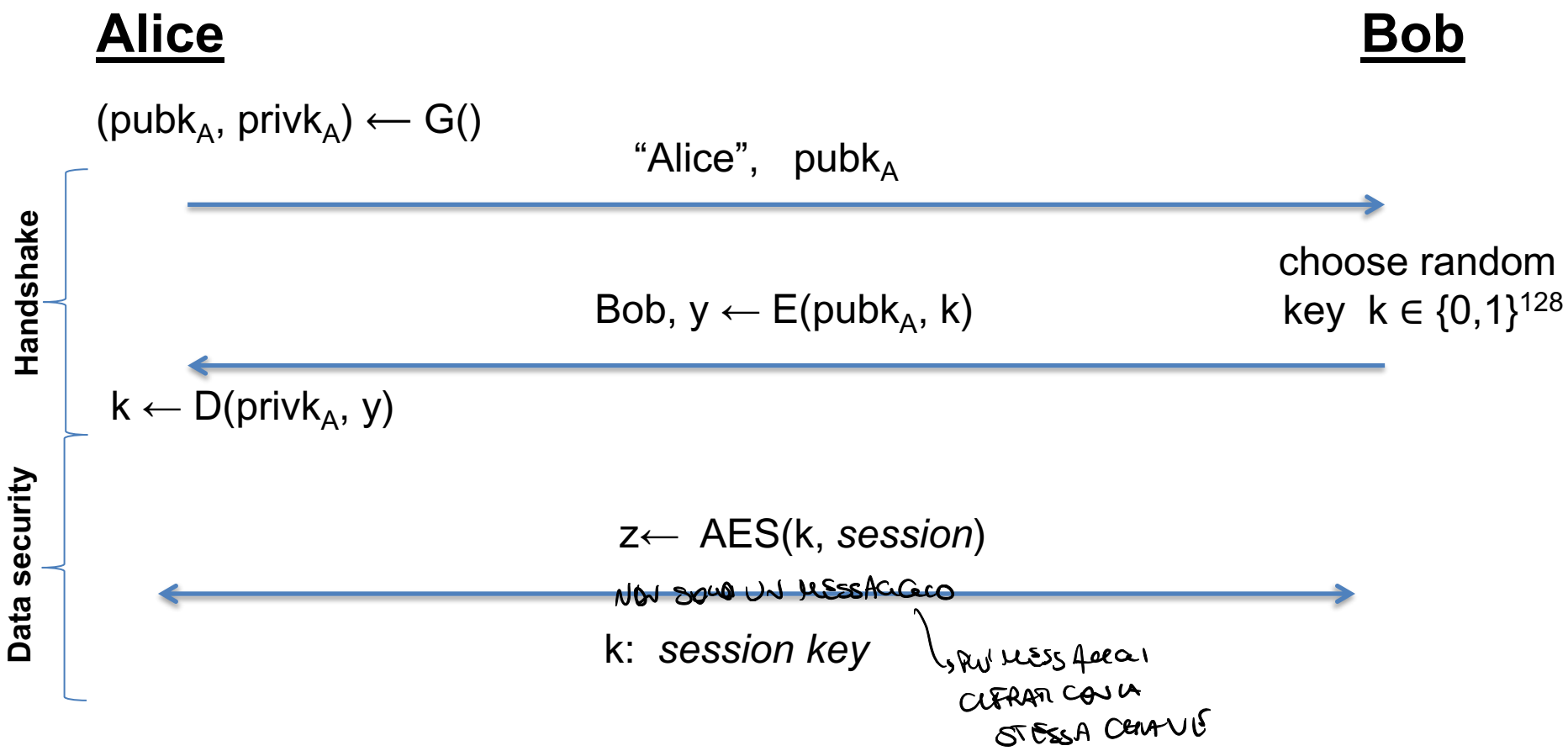
- Public key cryptography is 2-3 orders of magnitude slower than symmetric key cryptography
  - Public-key performance can be a more serious bottleneck in constrained devices, e.g., mobile phones or smart cards, or on network servers that have to compute many public-key operations per second
- A digital envelope uses two layers for encryption:
  - Symmetric key encryption is used for message encryption and decryption.
  - Public key encryption is used to send symmetric key to the receiving party



Hybrid protocol: digital envelope



Basic key transport protocol



Families of pub key algs

- Built on the common principle of one-way function
- A function f() is a one-way function if:
  - $y = f(x)$ is computationally easy, and
  - $x = f^{-1}(y)$ is computationally infeasible
- Two popular one-way functions
  - Integer factorization
  - Discrete logarithm

Families of PK Cryptography

- Integer factorization schemes (mid 70s)
  - Most prominet scheme: RSA
- Discrete Logarithm Schemes (mid 70s)
  - Most prominet schemes: DHKE, ElGamal, DSA
- Elliptic Curves Schemes (mid 80s)
  - EC schemes are a generalization of the Discrete Logarithm algorithm
  - Most prominet schemes: ECDH, ECDSA

Families of PK Cryptography

- Other schemes
  - Multivariate Quadratic, Lattice
    - They lack maturity
    - Poor performance characteristics
  - Hyperelliptic curve cryptosystems
    - Secure and efficient
    - They have not gained widespread adoption

Main security mechanisms

- Key establishment
  - Establishing keys over an insecure channel
  - DHKE, RSA key transport
- Non repudiation and message integrity
  - Digital signatures
  - RSA, DSA, ECDSA
- Identification
  - Challenge-response protocol together digital signatures
- Encryption
  - RSA and ElGamal

Key Lenghts and Security Level

- An algorithm has *security level* of n bit, if the best known algorithm requires 2^n steps
- Symmetric algorithms with security level of n have a key of length of n bits
- In asymmetric algorithms, the relationship between security level and cryptographic strengh is no at straightforward

Key Lenghts and Security Level

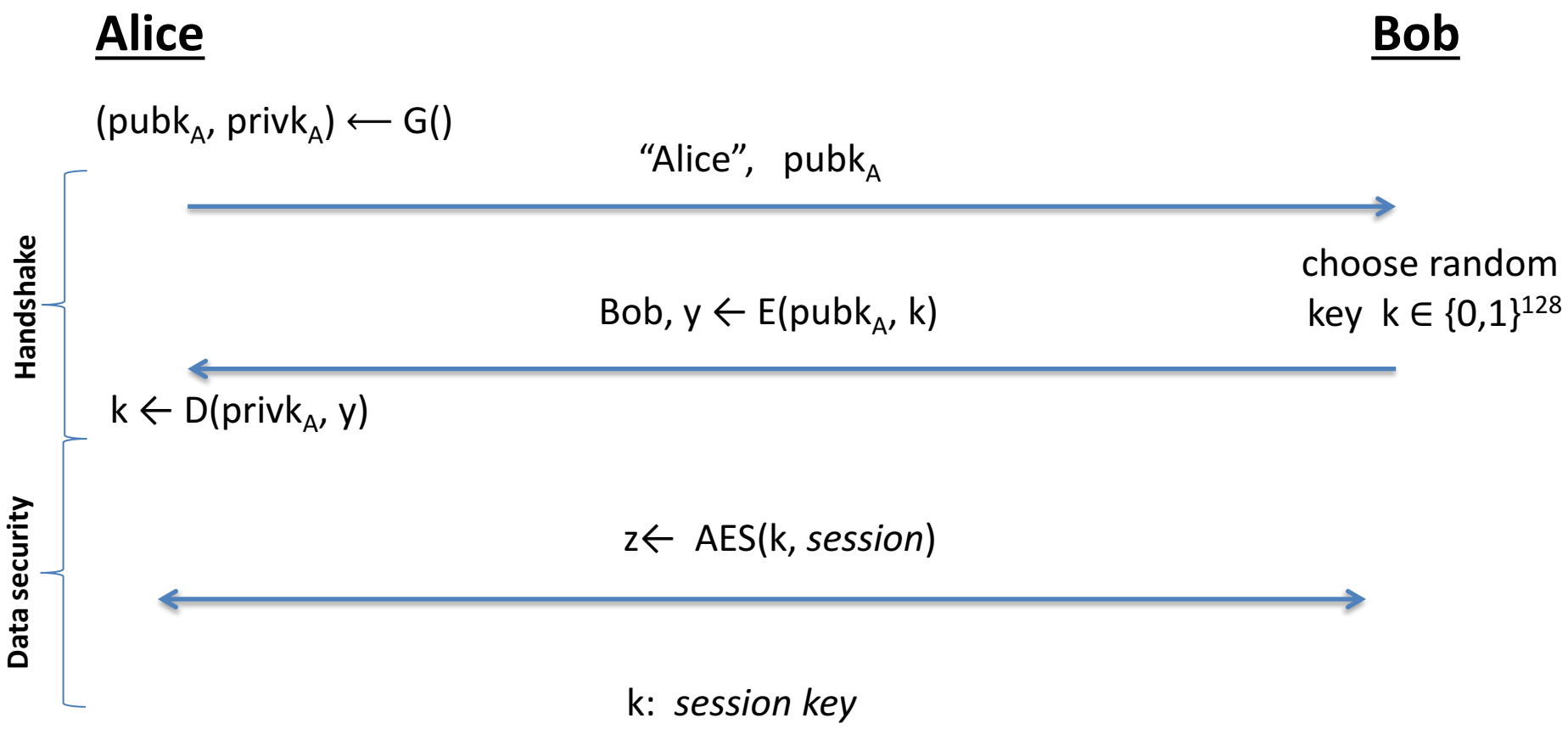
Algorithm Family	Cryptosystem	Security Level			
		80	128	192	256
Integer Factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete Logarithm	DH, DSA, ElGamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric key	AES, 3DES	80 bit	128 bit	192 bit	256 bit

RULE OF THUMB - The computational complexity of the three public key algorithm families grows roughly with the cube bit length

Public Key Cryptography

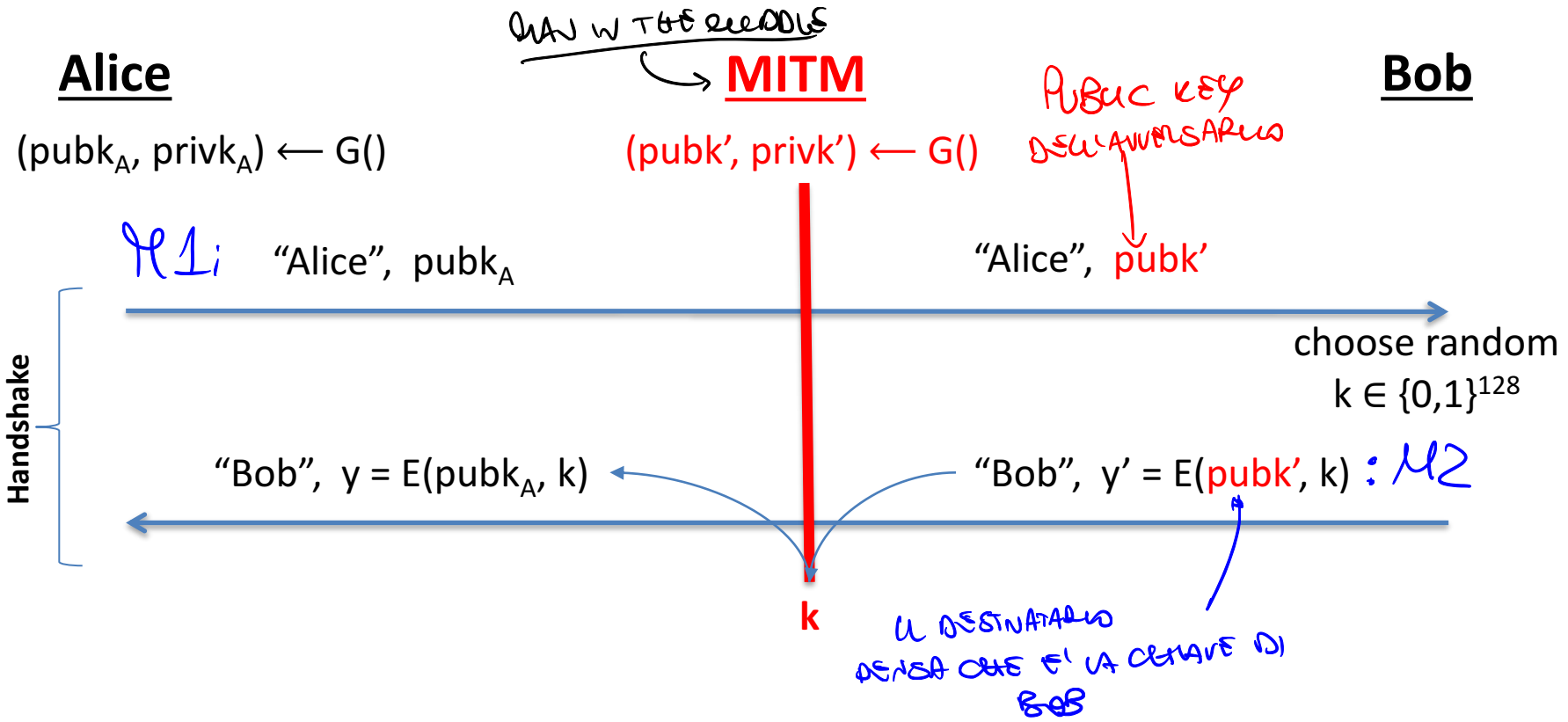
KEY AUTHENTICATION

Basic key transport protocol

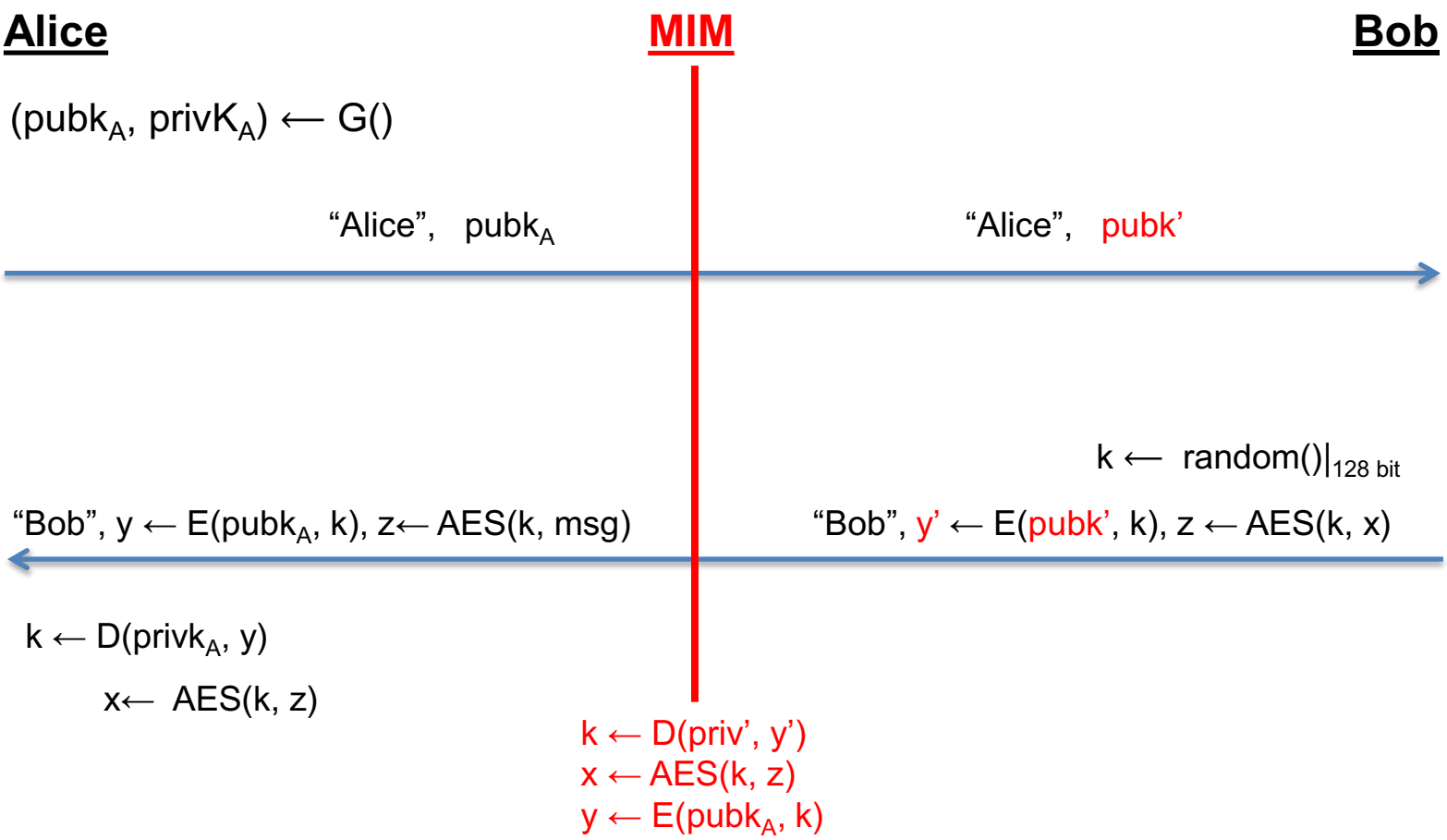


Man-in-the-middle (MIM) attack

The protocol is insecure against **active** attacks



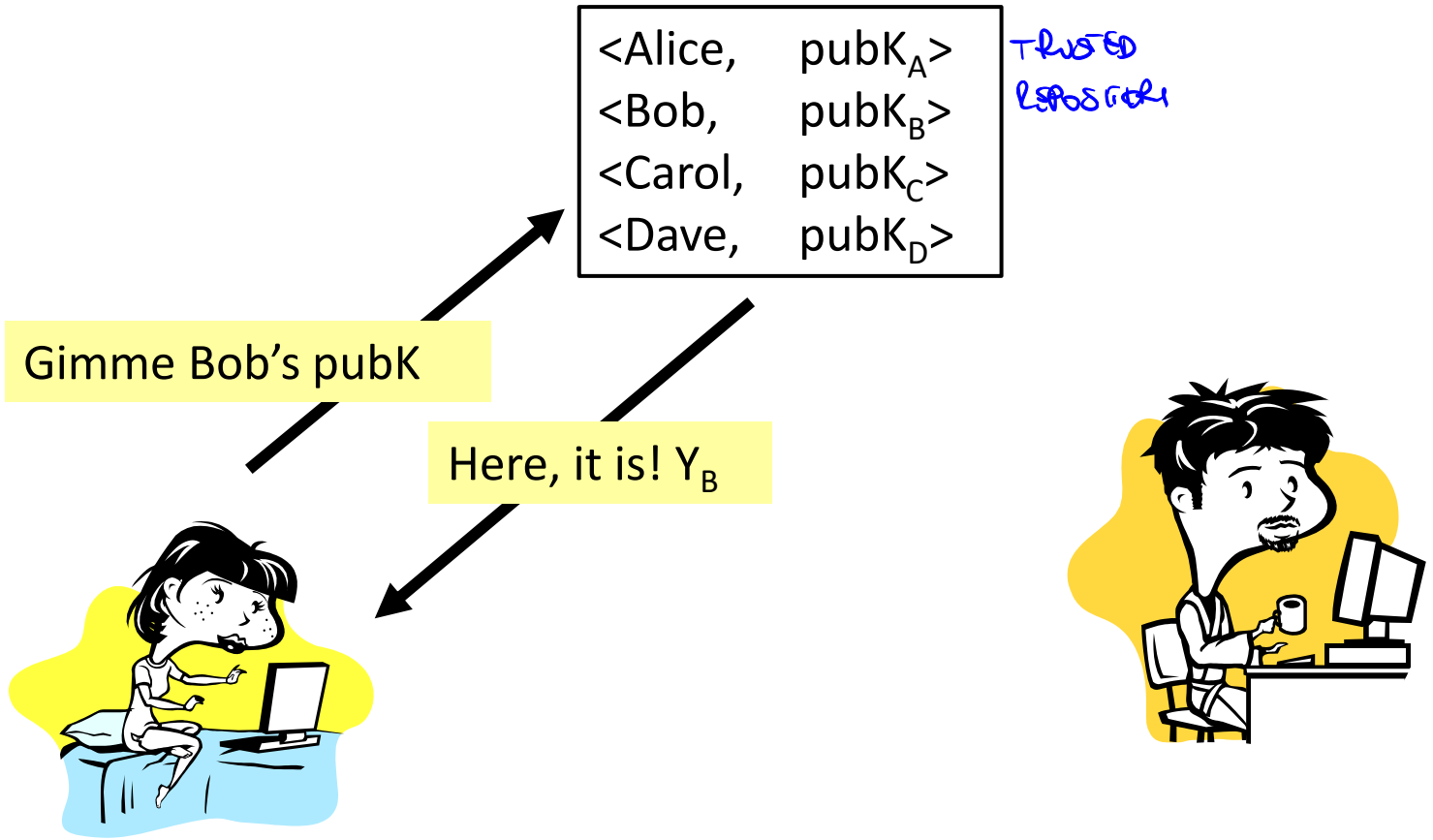
MIM attack against digital envelope



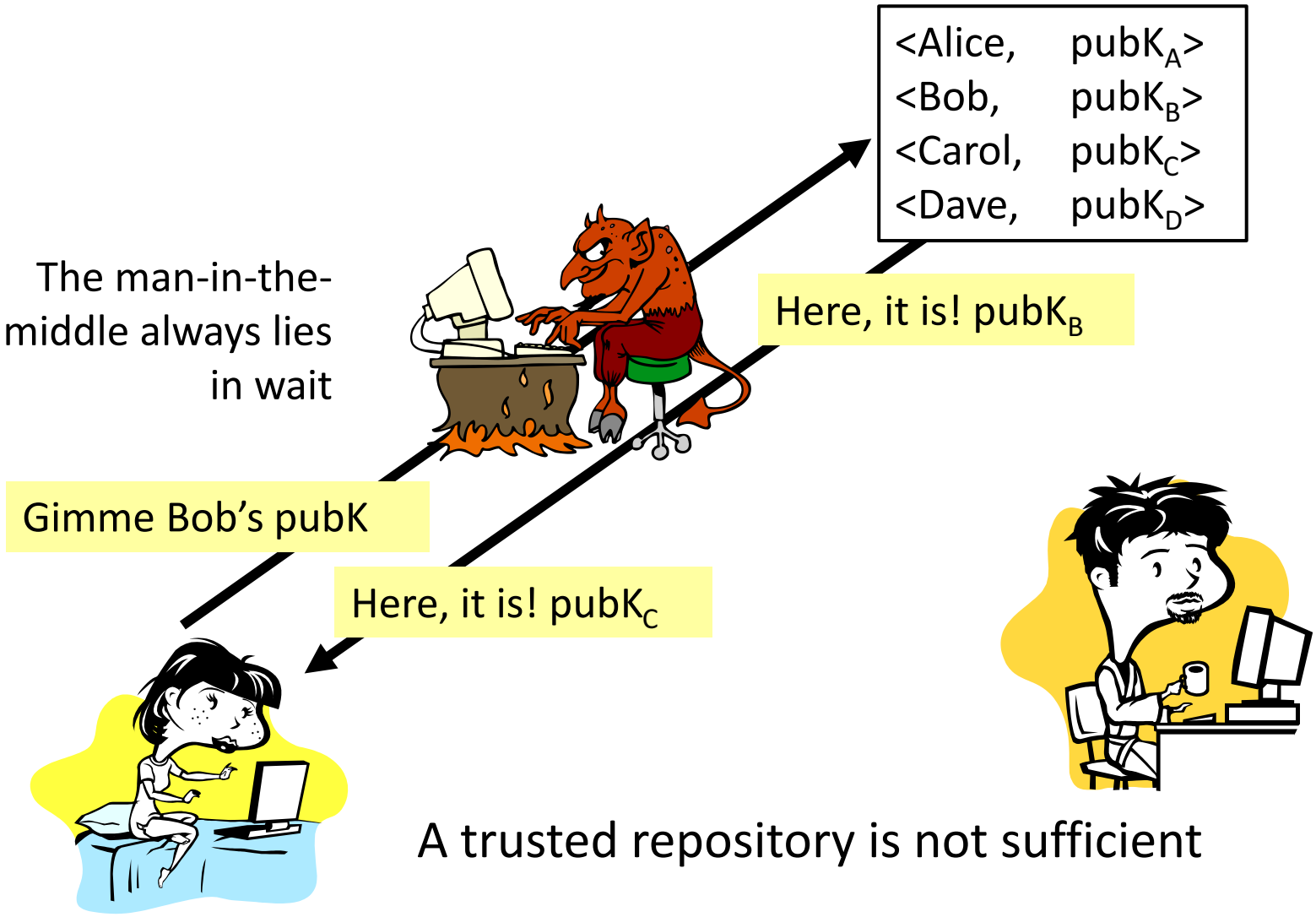
A trusted repository (I)

UNIVERSITÀ DI PISA

Public read-only repository trusted to preserve the integrity of the pairs <identifier, public key>



A trusted repository (II)



A trusted repository is not sufficient

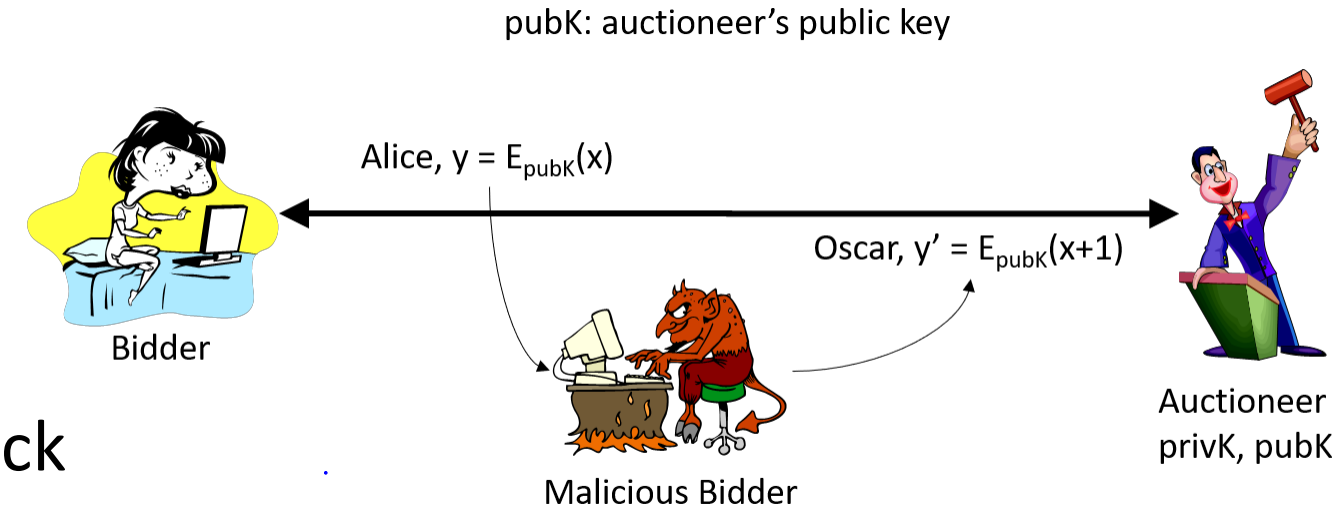
Key authentication

- MIM attack is an active attack
- Lack of key authentication makes MIM possible
- Certificates are a solution

Public Key Cryptography

PLAINTEXT RANDOMIZATION

Attack against a small plaintex space

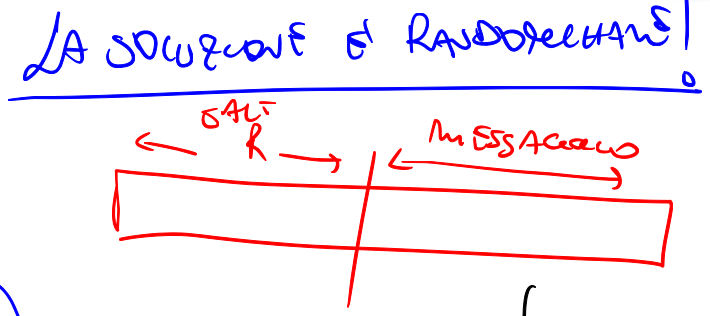


- The attack
  - Intercept y
  - Try all the possible x's until find x* such that y = $E_{pubK}(x^*)$, then x* == x
  - Let x' = x* + 1
  - Send y' = $E_{pubK}(x')$

Attack against a small plaintex space

- Attack complexity
  - If bid x is an integer, then up to 2^{32} attempts
  - If bid x $\in [x_{min}, x_{max}]$, then #attempts $\ll 2^{32}$

Attack against a small plaintex space



- Countermeasure: salting
  - Bidder side
    - Salt $s \leftarrow \text{random}()|_{\text{r-bit}}$
    - Bid $b \leftarrow (s, x)$
    - $y = E_{\text{pubK}}(b)$
  - Auctioneer side
    - $(s, x) \leftarrow D_{\text{privK}}(b)$ and retain x
  - Adversary
    - Try alle the possible pairs (bid, salt)
    - Attack complexits gets multiplied by 2^r