Public Key Encryption

Gianluca Dini
Dept. Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@unipi.it
Version: 11/03/2025

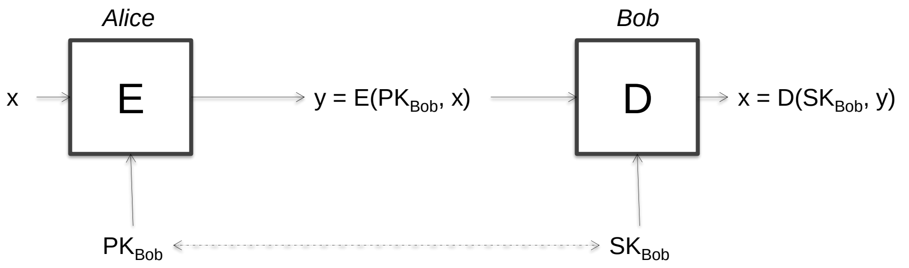
1

Public Key Cryptography

INTRODUCTION

2

Communication model



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

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 ∈ $\mathcal{M}$ and outputs y ∈ $\mathcal{C}$
  - x = **D**(sk, y) is deterministic alg. that takes y ∈ $\mathcal{C}$ and outputs x ∈ $\mathcal{M}$
  - fulfills the **Consistency Property**
    - $\forall$(pk, sk), $\forall$ x ∈ $\mathcal{M}$, D(sk, E(pk, x)) = x

PANKO OBSERVES

Security of PKE: informal

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

Non-randomized PKE is not perfect

Whereas a perfect cypher exists, same for block cyphers, but a PK scheme cannot

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

↓ a posteriori prob. is different from the a priori one.

PKE basic protocol

Naive use

UNIVERSITÀ DI PISA

Alice **Bob**

(pk, sk) ⟵ G()

"Alice", pk ⟶

Msg x

⟵ Bob, $y \leftarrow E_{pk}(x)$

$x \leftarrow D_{sk}(y)$

Insecure channel

Mar-25 Public Key Encryption 7

7

Digital envelope

UNIVERSITÀ DI PISA

- Public key cryptography is 2-3 orders of magnitude slower than symmetric key cryptography Unconvenient from performances POV
  - 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

Mar-25 Public Key Encryption 8

8

Hybrid protocol: digital envelope

UNIVERSITÀ DI PISA

Off-line method

Alice **Bob**

(pubk$_A$, privK$_A$) ⟵ G() ["Alice", pubk$_A$]

k ⟵ random()|$_{128\ bit}$

bob generates a symmetric key, encrypts message by means of key and encrypt key by means of alice key

Bob, y ← E(pubk$_A$, k), z ← AES(k, x)

k ← D(privk$_A$, y)
x← AES^{-1}(k, z)

PK enc is used on a very small amount of data (16 bytes).

Mar-25 Public Key Encryption 9

9

This method doesn't use shared secrets.

Basic key transport protocol

UNIVERSITÀ DI PISA

Alice **Bob**

(pubk$_A$, privk$_A$) ⟵ G()

Handshake

"Alice", pubk$_A$

choose random key k ∈ $\{0,1\}^{128}$

Bob, y ⟵ E(pubk$_A$, k)

k ⟵ D(privk$_A$, y)

Generalised

Data security

AES(k, *session*)

k: *session key*
Disclaimer: toy protocol!

Mar-25 Public Key Encryption 10

10

Public Key Encryption

PUBLIC KEY CRYPTOGRAPHY

11

Families of pub key algs

UNIVERSITÀ DI PISA

- 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

Cyphers are not one way functions

- Two popular one-way functions
  - Integer factorization
  - Discrete logarithm [log in a subset of nrs]

12

Families of PK Cryptography

UNIVERSITÀ DI PISA

- Integer factorization schemes (mid 70s)
  - Most prominent scheme: RSA
- Discrete Logarithm Schemes (mid 70s)
  - Most prominent schemes: DHKE, ElGamal, DSA

    invented algorithm for DS

    Diffie Hellman Key establishment
- Elliptic Curves Schemes (mid 80s)
  - EC schemes are a generalization of the Discrete Logarithm algorithm
  - Most prominent schemes: ECDH, ECDSA

Completely broken by quantum attacks

Families of PK Cryptography

UNIVERSITÀ DI PISA

- Other schemes
  - Multivariate Quadratic, Lattice

    PK schemes based on lattices seem to be resistant to quantum computing
    - They lack maturity
    - Poor performance characteristics
  - Hyperelliptic curve cryptosystems
    - Secure and efficient
    - They have not gained widespread adoption

Main security mechanisms

- Encryption
  - RSA and ElGamal
- 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

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 as 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 of bit length

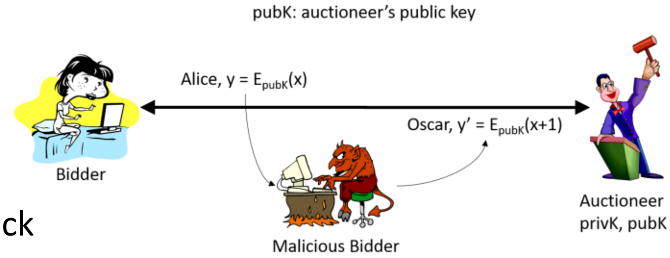
17

Public Key Cryptography

THE NEED FOR ENCRYPTION RANDOMIZATION

18

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' = $E_{pubK}(x')$

Mar-25 Public Key Encryption 19

19

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 $\ll 2^{32}$

Mar-25 Public Key Encryption 20

20

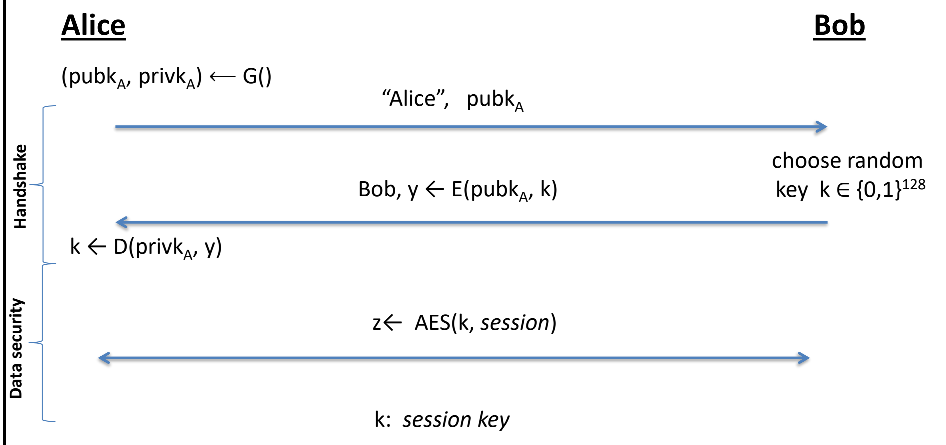
Attack against a small plaintex space

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

Public Key Cryptography

KEY AUTHENTICATION

Basic key transport protocol

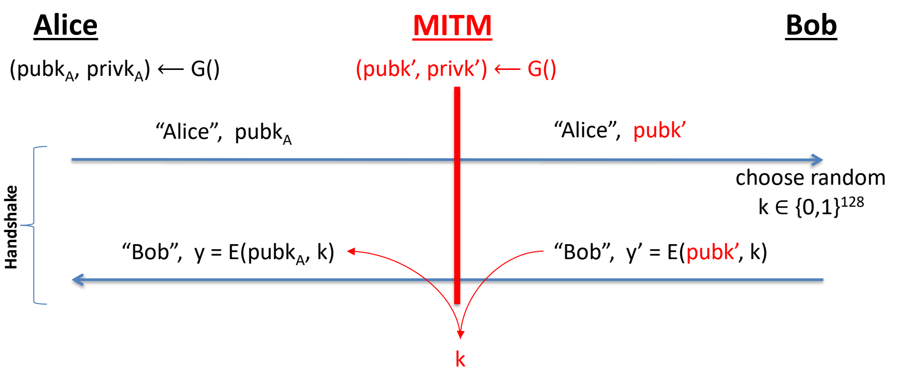


Mar-25 Public Key Encryption 23

23

Man-in-the-middle (MIM) attack

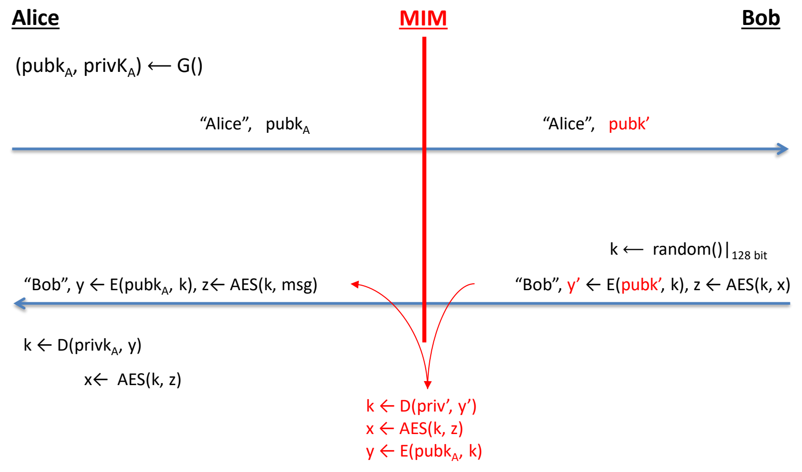
The protocol is insecure against **active** attacks



Mar-25 Public Key Encryption 24

24

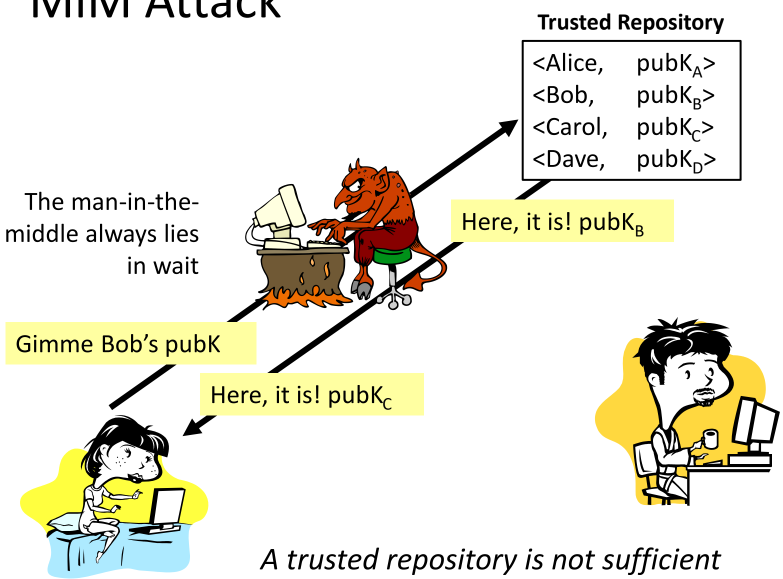
MIM attack against digital envelope



Mar-25 Public Key Encryption 25

25

MiM Attack



A trusted repository is not sufficient

Mar-25 Public Key Encryption 27

27

MiM attack vs key authentication

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