Public Key Cryptography

Gianluca Dini
Dept. Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@unipi.it

Version: 2022-04-12

1

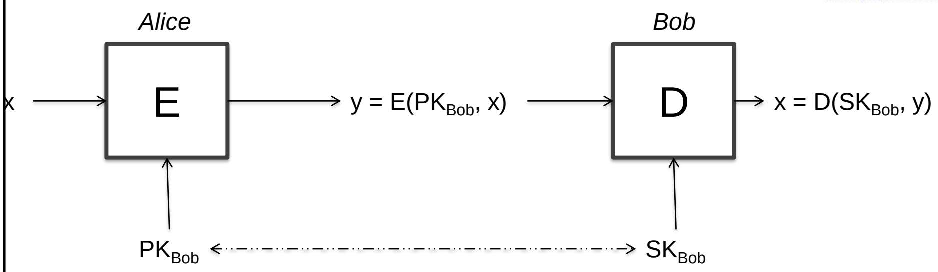
Public Key Cryptography

INTRODUCTION

Apr-22 Public-Key Encryption 2

2

Public key encryption



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

Apr-22 Public-Key Encryption 5

5

PKE is not perfect

- 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')
      - If y' == y then x' = x and Pr[M=x' | C=y] = 1
        else Pr[M=x' | C=y] = 0 (a posteriori)

Apr-22 Public-Key Encryption 6

6

PKE basic protocol

UNIVERSITÀ DI PISA

Alice **Bob**

(pk, sk) ← G()

"Alice", pk →

Msg x

Bob, y ← E(pk, x) ←

x ← D(sk, y)

Insecure channel

Apr-22 Public-Key Encryption 7

7

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

Apr-22 Public-Key Encryption 8

8

Hybrid protocol: digital envelope

UNIVERSITÀ DI PISA

Alice Off-line method **Bob**

$(pubk_A, privK_A) \leftarrow G()$

["Alice", $pubk_A$]

$k \leftarrow random()|_{128\ bit}$

Bob, $y \leftarrow E(pubk_A, k)$, $z \leftarrow AES(k, x)$

$k \leftarrow D(privk_A, y)$

$x \leftarrow AES(k, z)$

Apr-22 Public-Key Encryption 9

9

Basic key transport protocol

UNIVERSITÀ DI PISA

Alice **Bob**

$(pubk_A, privk_A) \leftarrow G()$

Handshake

"Alice", $pubk_A$

choose random key $k \in \{0,1\}^{128}$

Bob, $y \leftarrow E(pubk_A, k)$

$k \leftarrow D(privk_A, y)$

Data security

AES(k, *session*)

k: *session key*

Apr-22 Public-Key Encryption 10

10

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

11

Families of PK Cryptography

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

12

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

UNIVERSITÀ DI PISA

- 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

Apr-22 Public-Key Encryption 15

15

Key Lenghts and Security Level

UNIVERSITÀ DI PISA

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

Apr-22 Public-Key Encryption 16

16

Public Key Cryptography

KEY AUTHENTICATION

Apr-22 Public-Key Encryption 17

17

Basic key transport protocol

UNIVERSITÀ DI PISA

Alice **Bob**

(pubk$_A$, privk$_A$) $\longleftarrow$ G()

Handshake

“Alice”, pubk$_A$ $\longrightarrow$

choose random key k $\in \{0,1\}^{128}$

$\longleftarrow$ Bob, y $\leftarrow$ E(pubk$_A$, k)

k $\leftarrow$ D(privk$_A$, y)

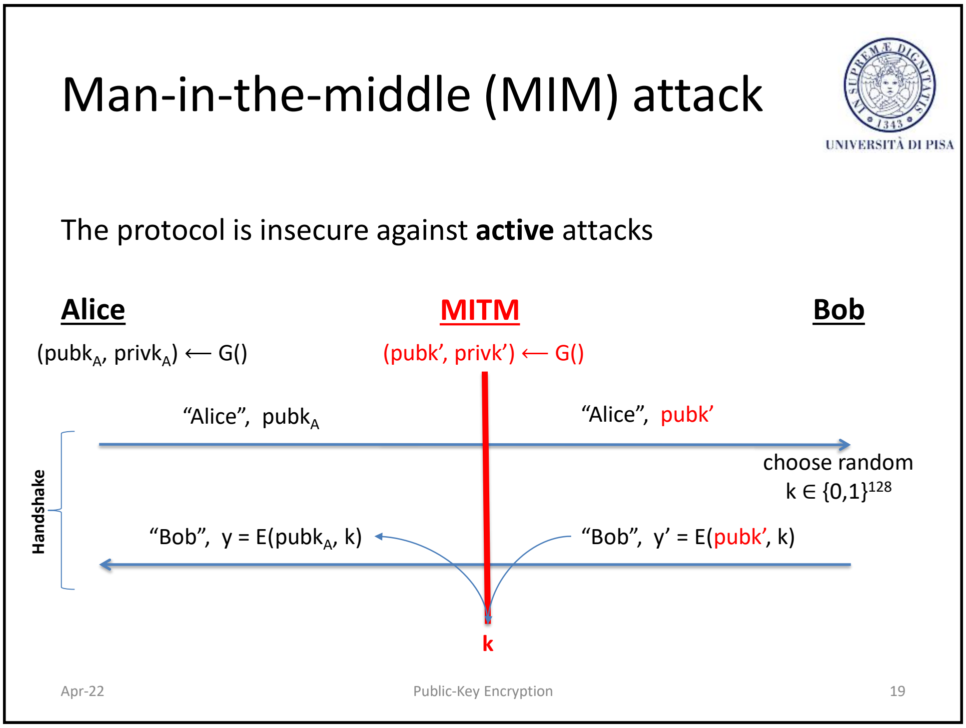
Data security

z$\leftarrow$ AES(k, *session*) $\longleftrightarrow$

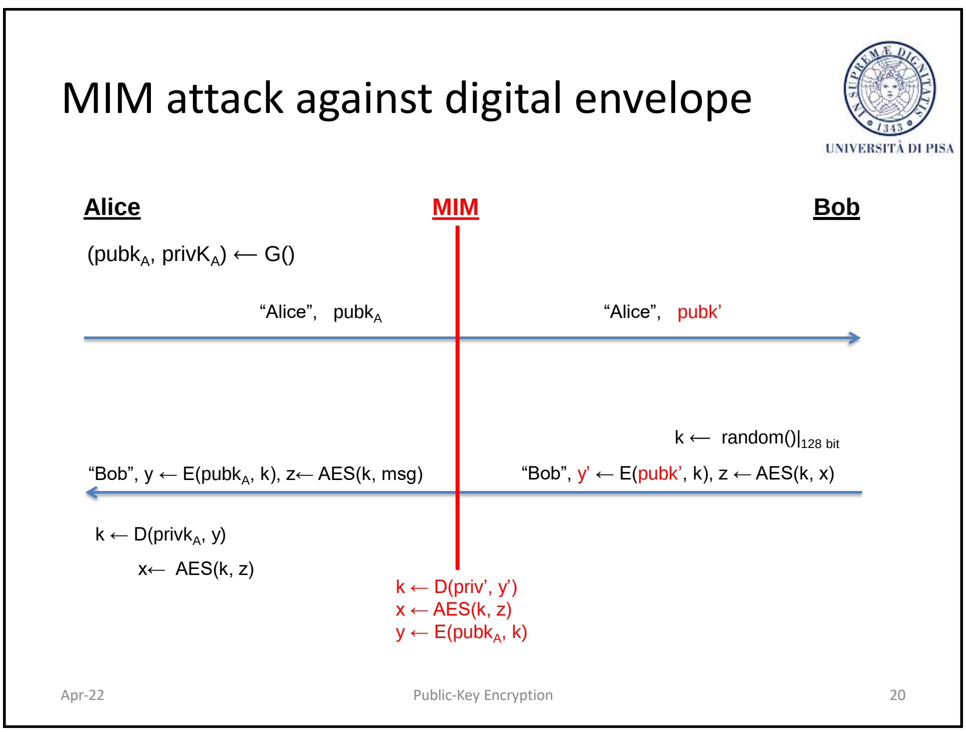
k: *session key*

Apr-22 Public-Key Encryption 18

18


Man-in-the-middle (MIM) attack
UNIVERSITÀ DI PISA
The protocol is insecure against **active** attacks
Alice
MITM
Bob
$(pubk_A, privk_A) \longleftarrow G()$
$(pubk', privk') \longleftarrow G()$
"Alice", $pubk_A$
"Alice", pubk'
Handshake
choose random
$k \in \{0,1\}^{128}$
"Bob", $y = E(pubk_A, k)$
"Bob", $y' = E(pubk', k)$
k
Apr-22
Public-Key Encryption
19

19


MIM attack against digital envelope
UNIVERSITÀ DI PISA
Alice
MIM
Bob
$(pubk_A, privK_A) \longleftarrow G()$
"Alice", $pubk_A$
"Alice", pubk'
$k \longleftarrow random()|_{128\ bit}$
"Bob", $y \leftarrow E(pubk_A, k)$, $z \leftarrow AES(k, msg)$
"Bob", $y' \leftarrow E(pubk', k)$, $z \leftarrow AES(k, x)$
$k \leftarrow D(privk_A, y)$
$x \leftarrow AES(k, z)$
$k \leftarrow D(priv', y')$
$x \leftarrow AES(k, z)$
$y \leftarrow E(pubk_A, k)$
Apr-22
Public-Key Encryption
20

20

A trusted repository (I)

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

<Alice,	$pubK_A$>
<Bob,	$pubK_B$>
<Carol,	$pubK_C$>
<Dave,	$pubK_D$>

Gimme Bob's pubK

Here, it is! Y_B

Apr-22 Public-Key Encryption 21

21

A trusted repository (II)

<Alice,	$pubK_A$>
<Bob,	$pubK_B$>
<Carol,	$pubK_C$>
<Dave,	$pubK_D$>

The man-in-the-middle always lies in wait

Here, it is! $pubK_B$

Gimme Bob's pubK

Here, it is! $pubK_C$

A trusted repository is not sufficient

Apr-22 Public-Key Encryption 22

22

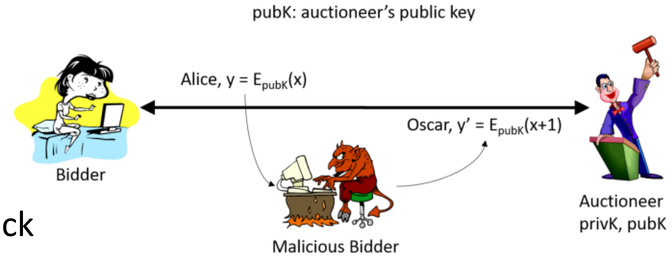
Key authentication

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

Public Key Cryptography

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

25

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 $\ll 2^{32}$

26

Attack against a small plaintex space

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