



Public Key Encryption

Gianluca Dini
Dept. Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@unipi.it
Version: 2024-03-13

1

Public Key Cryptography


INTRODUCTION

Mar-24

Public Key Encryption

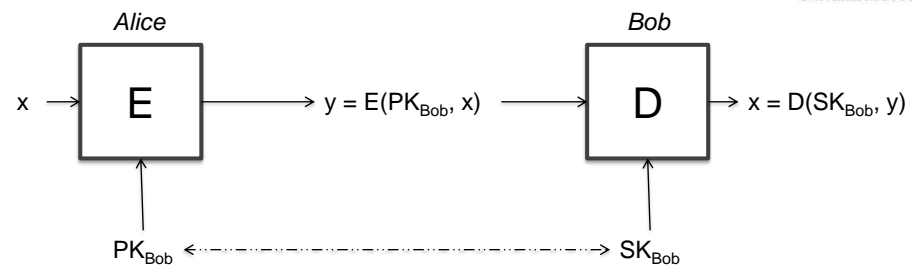
2

2



UNIVERSITÀ DI PISA

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 $privK_{Bob}$

Mar-24

Public Key Encryption

3

3



UNIVERSITÀ DI PISA

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*
 - $\forall (pk, sk), \forall x \in M, D(sk, E(pk, x)) = x$

Mar-24

Public Key Encryption

4

4

Security of PKE: informal



UNIVERSITÀ DI PISA

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

Mar-24

Public Key Encryption

5

5

Non-randomized 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
 - selects x' s.t. $\Pr[M = x'] \neq 0$ (a priori)
 - computes $y' = E_{pk}(x')$
 - If $y' = y$ then $x' = x$ and $\Pr[M=x' \mid C=y] = 1$
else $\Pr[M=x' \mid C=y] = 0$ (a posteriori)

Mar-24

Public Key Encryption

6

6



UNIVERSITÀ DI PISA

PKE basic protocol

Alice

$(pk, sk) \leftarrow G()$

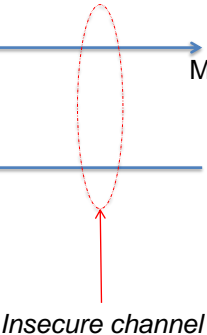
Bob

“Alice”, pk

Msg x

Bob, $y \leftarrow E_{pk}(x)$

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




Insecure channel

Mar-24

Public Key Encryption

7

7



UNIVERSITÀ DI PISA

Digital envelope

- 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


Mar-24

Public Key Encryption

8

8

Hybrid protocol: digital envelope



UNIVERSITÀ DI PISA

Alice

$(\text{pubk}_A, \text{privK}_A) \leftarrow G()$

Bob

$["\text{Alice}", \text{pubk}_A]$

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

Off-line method

Bob, $y \leftarrow E(\text{pubk}_A, k), z \leftarrow \text{AES}(k, x)$

$k \leftarrow D(\text{privk}_A, y)$


$x \leftarrow \text{AES}(k, z)$

Mar-24

Public Key Encryption

9

Basic key transport protocol



UNIVERSITÀ DI PISA

Alice

$(\text{pubk}_A, \text{privk}_A) \leftarrow G()$

Bob

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

Handshake

"Alice", pubk_A

Bob, $y \leftarrow E(\text{pubk}_A, k)$

$k \leftarrow D(\text{privk}_A, y)$

Data security

$\text{AES}(k, \text{session})$

k : session key

Mar-24

Public Key Encryption

10

Public Key Encryption

PUBLIC KEY CRYPTOGRAPHY


Mar-24

Public Key Encryption

11

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
- Two popular one-way functions
 - Integer factorization
 - Discrete logarithm

Mar-24

Public Key Encryption

12

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

Mar-24

Public Key Encryption

13

13

Families of PK Cryptography



UNIVERSITÀ DI PISA

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

Mar-24

Public Key Encryption

14

14

Main security mechanisms



UNIVERSITÀ DI PISA

- 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

Mar-24

Public Key Encryption

15

15

Key Lengths 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 strength is not as straightforward


Mar-24

Public Key Encryption

16

16

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 of bit length

Mar-24

Public Key Encryption

17

17

Public Key Cryptography

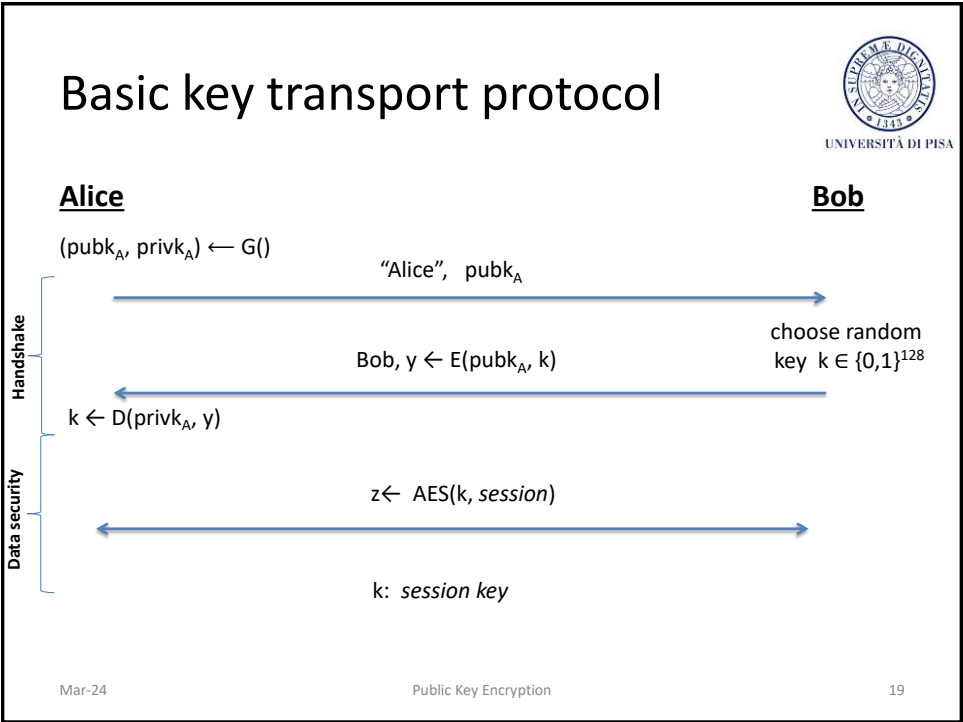
KEY AUTHENTICATION

Mar-24

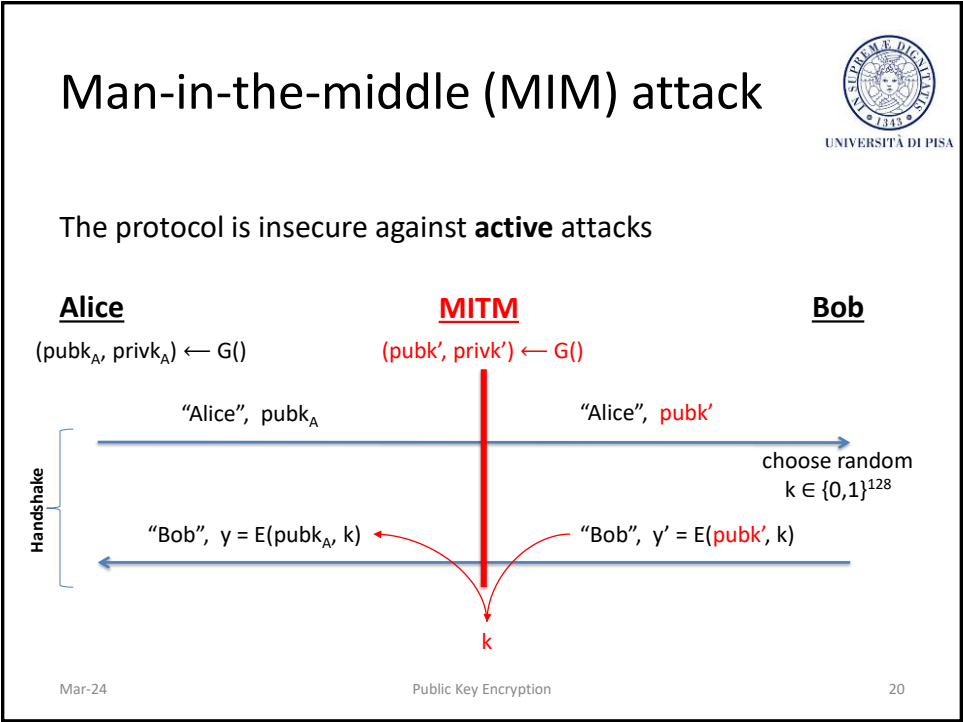
Public Key Encryption

18


18



19



20


UNIVERSITÀ DI PISA

MIM attack against digital envelope

Alice

$(\text{pubk}_A, \text{privK}_A) \leftarrow G()$

"Alice", pubk_A

"Bob", $y \leftarrow E(\text{pubk}_A, k), z \leftarrow \text{AES}(k, \text{msg})$

$k \leftarrow D(\text{privK}_A, y)$

$x \leftarrow \text{AES}(k, z)$

MIM

$k \leftarrow D(\text{priv}', y')$

$x \leftarrow \text{AES}(k, z)$

$y \leftarrow E(\text{pubk}_A, k)$

Bob

"Alice", pubk'

$k \leftarrow \text{random}() \upharpoonright_{128 \text{ bit}}$


"Bob", $y' \leftarrow E(\text{pubk}', k), z \leftarrow \text{AES}(k, x)$

Mar-24

Public Key Encryption

21

21


UNIVERSITÀ DI PISA

MiM Attack

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

Gimme Bob's pubK

Here, it is! pubK_C

Here, it is! pubK_B

Trusted Repository

$\langle \text{Alice}, \text{pubK}_A \rangle$

$\langle \text{Bob}, \text{pubK}_B \rangle$

$\langle \text{Carol}, \text{pubK}_C \rangle$

$\langle \text{Dave}, \text{pubK}_D \rangle$

A trusted repository is not sufficient

Mar-24

Public Key Encryption

23

23

MiM attack vs key authentication

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



UNIVERSITÀ DI PISA

Mar-24


Public Key Encryption

24

24

Public Key Cryptography

THE NEED FOR ENCRYPTION RANDOMIZATION



UNIVERSITÀ DI PISA

Mar-24

Public Key Encryption

25

25

Attack against a small plaintext space

pubK: auctioneer's public key

Alice, $y = E_{\text{pubK}}(x)$

Bidder

Malicious Bidder

Oscar, $y' = E_{\text{pubK}}(x+1)$

Auctioneer privK, pubK

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

Mar-24 Public Key Encryption 26

Attack against a small plaintext space

UNIVERSITÀ DI PISA

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

Mar-24 Public Key Encryption 27

Attack against a small plaintext space



- Countermeasure: salting
 - Bidder side
 - Salt $s \leftarrow \text{random}() \mid_{r\text{-bit}}$
 - Bid $b \leftarrow (s, x)$
 - $y = E_{\text{pubk}}(b)$
 - Auctioneer side
 - $(s, x) \leftarrow D_{\text{privk}}(b)$ and retain x
 - Adversary
 - Try all the possible pairs (bid, salt)
 - Attack complexity gets multiplied by 2^r

Mar-24

Public Key Encryption

28

28