Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Asymmetric encryption

Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services *(www.bydesign-project.eu)*

This presentation has been based on material provided by Dr. K. Limniotis (HDPA)

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

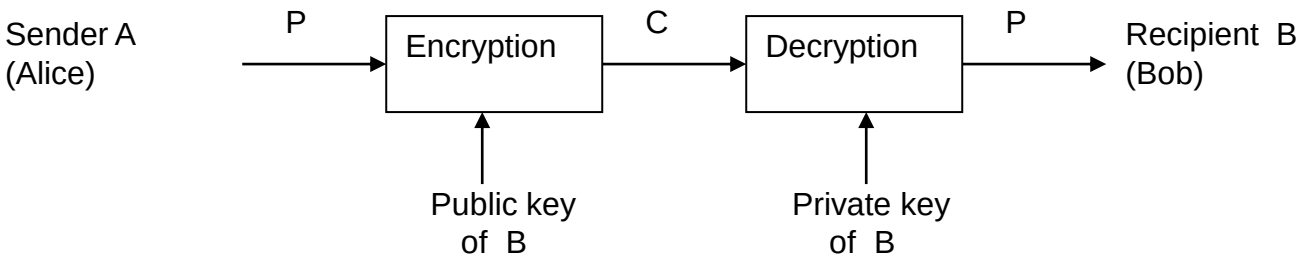
Public-Key Cryptography

- Probably most significant advance in the 3000 year history of cryptography
- uses two keys – a public & a private key
- Asymmetric since parties are not equal
- uses clever application of mathematical (mainly number theoretic) concepts to function
- Note: complements rather than replaces symmetric key crypto

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Public key encryption - operation

- Public-key (or asymmetric) encryption/decryption involves the use of two keys:
  - a public-key, which may be known by anybody (including adversaries), and can be used to encrypt messages,
  - a related private-key, known only to the recipient, used to decrypt messages,
  - infeasible to determine private key from public
- is asymmetric because
  - those who encrypt messages cannot decrypt these messages – only the legitimate recipient can



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

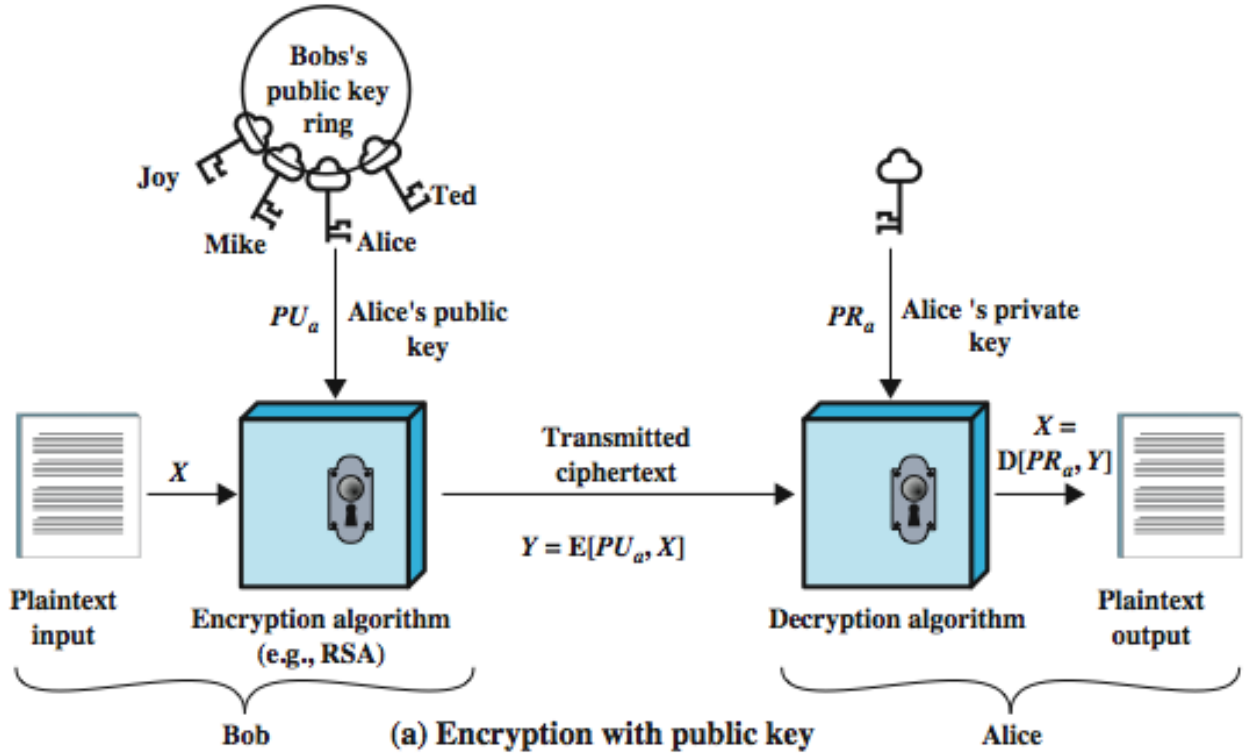
Why Public-Key Cryptography?

- The sender may start encryption without any prior “secret” communication with the recipient
  - The secure key distribution problem is being solved
  - As it will be shown next, public-key crpytography also suffices to generate digital signatures – used to verify a message comes intact from the claimed sender
- Public invention due to Whitfield Diffie & Martin Hellman at Stanford University in 1976
  - Seems though to be known earlier in classified community
  - Diffie and Hellman, received the 2015 Turing award - http://awards.acm.org/about/2015-turing

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Public-Key Cryptography – a more generalized view

- The sender has a ring of public keys, (at least) one for each potential recipient
- Of course, the sender has also his own public-private key pair…



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Symmetric vs Public-Key

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Some widely known public key cryptographic schemed

- Diffie-Hellman (protocol)
- RSA
- El Gamal
- Rabin
- McEliece
- Elliptic curve cryptography
- And others…

- Not all of them are being used for the same purposes

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Public-Key Applications

- can be classifies into 3 categories:
  - encryption/decryption (provide secrecy)
  - digital signatures (provide authentication)
  - key exchange (of session keys)
- some algorithms are suitable for all uses, others are specific to one

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

RSA

- by Rivest, Shamir & Adleman of MIT in 1977
- best known & widely used public-key scheme
- based on exponentiation in a finite field over integers modulo a prime
- uses large integers (eg. 2048 bits today)
- security due to cost of factoring large numbers

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ασφάλεια και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Which is the difficult mathematical problem for RSA?

- Any positive integer n can be represented in exactly one way as a product of primes (Fundamental Theorem of Arithmetic)
  - e.g. $140 = 2 \cdot 2 \cdot 5 \cdot 7$
  - There is no other product of primes which gives rise to 140
- Finding out the unique such product of primes, for given number n, is being called factorization of n
- Factorization is known to be computationally hard
- The security of RSA is based on the difficulty of the factorization problem

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Length of an RSA modulus

- It is hard to compare the equivalent security parameters for symmetric key cipher systems and RSA, however it is roughly believed that factorising a 512 bit number is about as hard as searching for a 56 bit symmetric key.
- Today, 2048 bits provide security (NIST suggests 2048 bits for RSA modulus size) – corresponds to 112-bit key security

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

RSA Security

- Possible approaches to attacking RSA are:
  - brute force key search
    - infeasible given the large size of numbers
  - mathematical attacks
    - based on difficulty of computing φ(N), by factoring modulus N, or on not properly chosen parameters
  - timing attacks
    - on running of decryption
  - chosen ciphertext attacks
    - given properties of RSA

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Elliptic curve cryptography (ECC)

- A general class of public key algorithms that are based on a special mathematical structure, being called elliptic curve
  - Similarly to the DLP problem, there is a known difficult problem that is being called Elliptic Curve Discrete Logarithm Problem (ECDLP)
  - Any cipher whose security rests wit the difficulty of the ECDLP, is being called an elliptic curve cryptographic algorithm
  - ECC and RSA constitute the most common implementations of the public key algorithms
  - ECC will not be discussed in this course…

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

The major advantage of the ECC

- Smaller key sizes to achieve the same level of security

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

General advantages of public key cryptographic algorithms

- No previous negotiation is needed
- The key pair can remain unchangeable for many years
  - In contrast to the symmetric key
- In a network, a much smaller number of keys is needed to be distributed with respect to the symmetric key
  - In symmetric encryption, we need a different key for each pair of users!
  - If we have N users, we actually need N(N-1)/2 symmetric keys

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

General disadvantages of public key cryptographic algorithms

- Much smaller throughput
  - Actually, we cannot encrypt real time communication with public key encryption
- Keys of large sizes are difficulty to be handled
- Their security rests with difficult mathematical problems which are known to be difficult but they have not proved to be “unsolvable”.
  - What if we find a “solution” for such a problem?
- In a post-quantum world, most public key algorithms will be no secure any more!!

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Combining symmetric with public key algorithms (1/3)

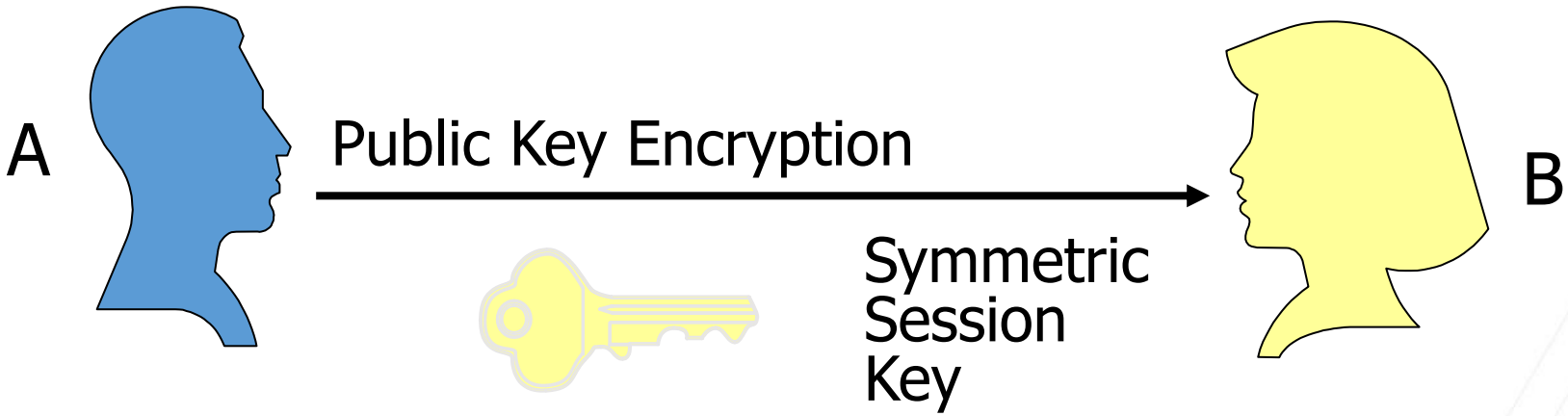
First, a mutual authentication needs to be performed,

- Public key cryptographic structures are being used

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Combining symmetric with public key algorithms (2/3)

- Next, a user generates a symmetric key
- This key is being encrypted with the public key of the other user and is being transmitted to her
  - Hence, they both have the same secret key, being securely interchanged



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Combining symmetric with public key algorithms (3/3)

- Now they communicate securely, with symmetric key encryption