Ασύμμετρη Κρυπτογραφία

Θεωρία και εφαρμογές

Αλέξανδρος Αφεντούλης
el06150 [at] mail.ntua.gr

Κοινότητα Ελεύθερου Λογισμικού ΕΜΠ
free and open source software community / national technical university of athens

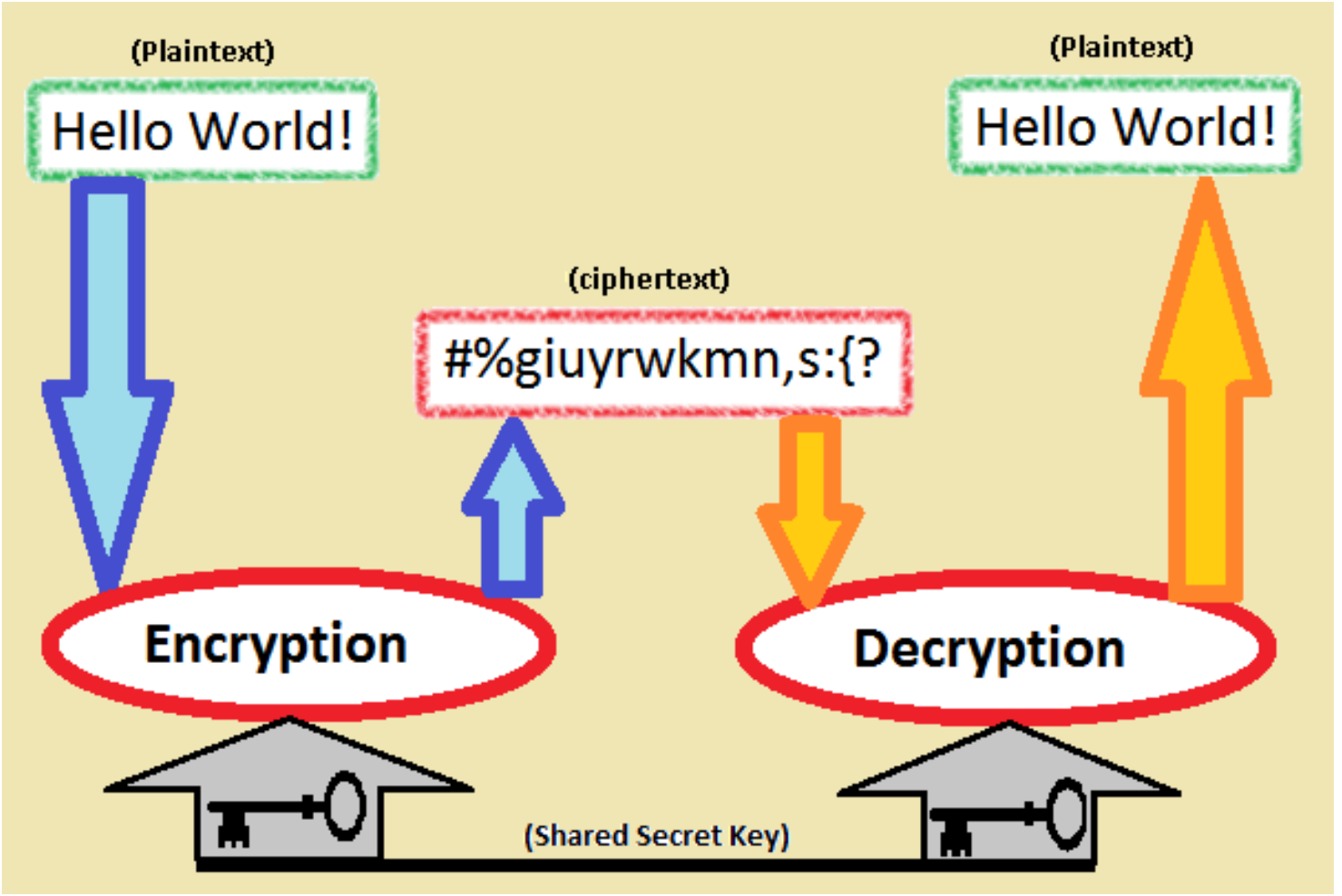
Λεξιλόγιο

- plaintext : το μήνυμα σε αναγνώσιμη για όλους μορφή
- ciphertext : το μήνυμα σε κρυπτογραφημένη μορφή
- encryption : μετασχηματισμός του plaintext σε ciphertext
- decryption : μετασχηματισμός του ciphertext σε plaintext
- cipher : ο αλγόριθμός encryption ή decryption
- key : το κλειδί που χρησιμοποιείται σε encryption ή/και decryption

Συμμετρική Κρυπτογραφία

- Οι άνθρωποι πρώτα συνέλαβαν και εφάρμοσαν την ιδέα της συμμετρικής κρυπτογραφίας
- Στη συμμετρική κρυπτογραφία το ίδιο κλειδί χρησιμοποιείται για encryption & decryption.
- Γνωστοί αλγόριθμοι:
    - του Καίσαρα (don't use it!)
    - AES, Blowfish, 3DES, Serpent, Twofish
- Ευρεία χρήση συμμετρικών αλγορίθμων στη μεταφορά και αποθήκευση δεδομένων
- Δεν είναι πάντα εύκολο/δυνατό να μοιραζόμαστε ένα shared secret key.

Symmetric encryption/decryption



ASymmetric Encryption

- or Public Key Crypto
- Diffie – Hellman key exchange (1976)
- RSA, Rivest, Shamir, Adleman (1977)
- PGP, Phil Zimmermann (1991)

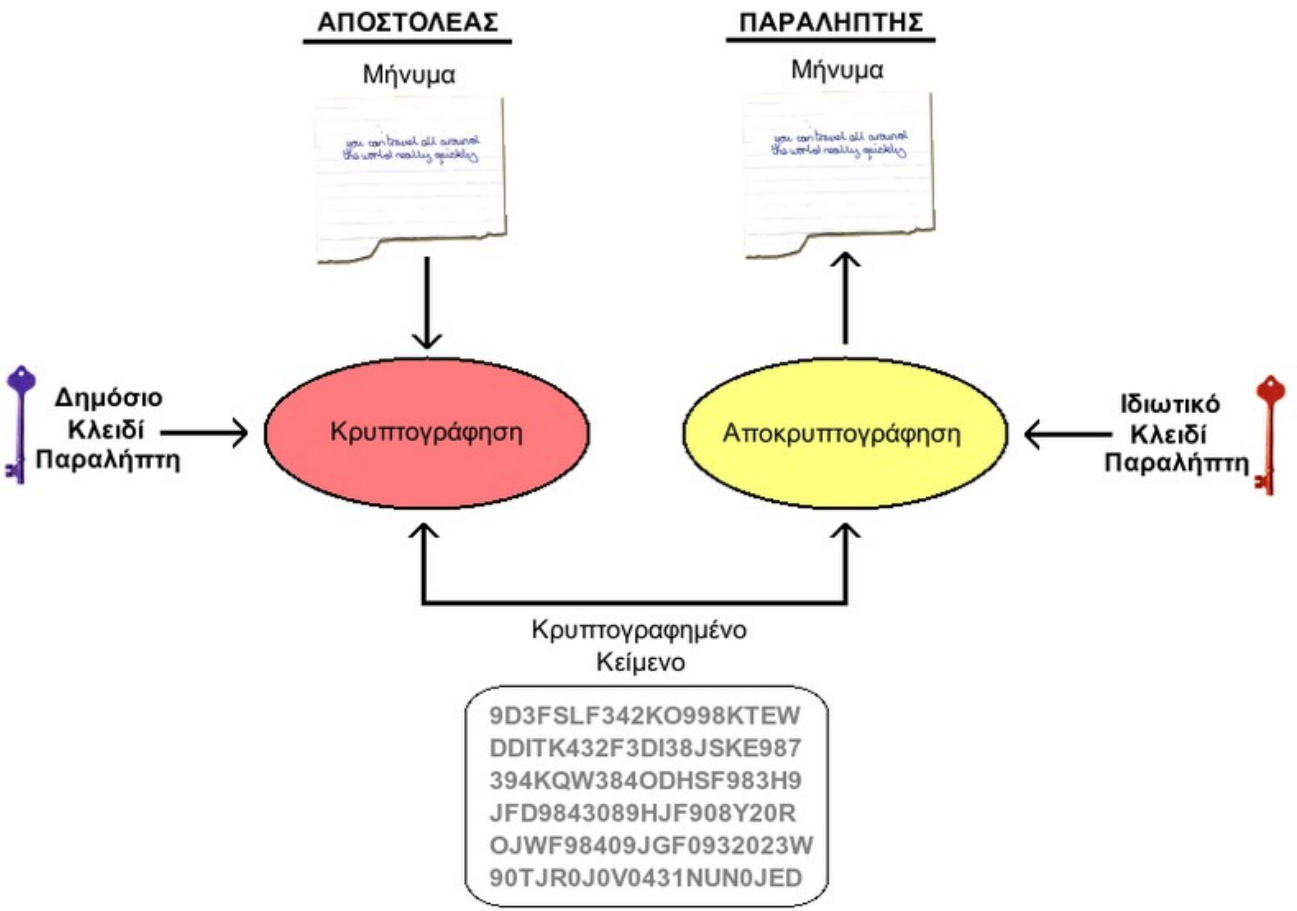
- Στόχος: Παράκαμψη της ανάγκης διαμοιρασμού ενός shared secret.
- Ιδέα: χρήση διαφορετικού κλειδιού σε encryption και decryption
- Βάση: προβλήματα που πιστεύουμε ότι δεν λύνονται γρήγορα, Prime Factorization, Discrete Logarithm, Elliptic Curves

- Γνωστοί αλγόριθμοι: ECDH, ECDSA, RSA, El-Gamal, SRP
- Πετυχαίνουμε : Data condidentiality (encryption), Data integrity and authenticity (signatures) or key exchange over insecure channel

Βασικές έννοιες

- **Εμπιστευτικότητα** (Confidentiality): Message should be readable only by entities having the decryption key (encryption/decryption).
- **Πιστοποίηση (**Authenticity): be able to verify who did send the message (digital signature)
- **Ακεραιότητα** (Integrity): be able to verify that the message did not change during transmission.
- **Κρυπτογράφηση απ' άκρη σ' άκρη** (end to end encryption): message is encrypted by the sender and decrypted by the receiver. No middle entity can access message's content.

ASymmetric Encryption/Decryption



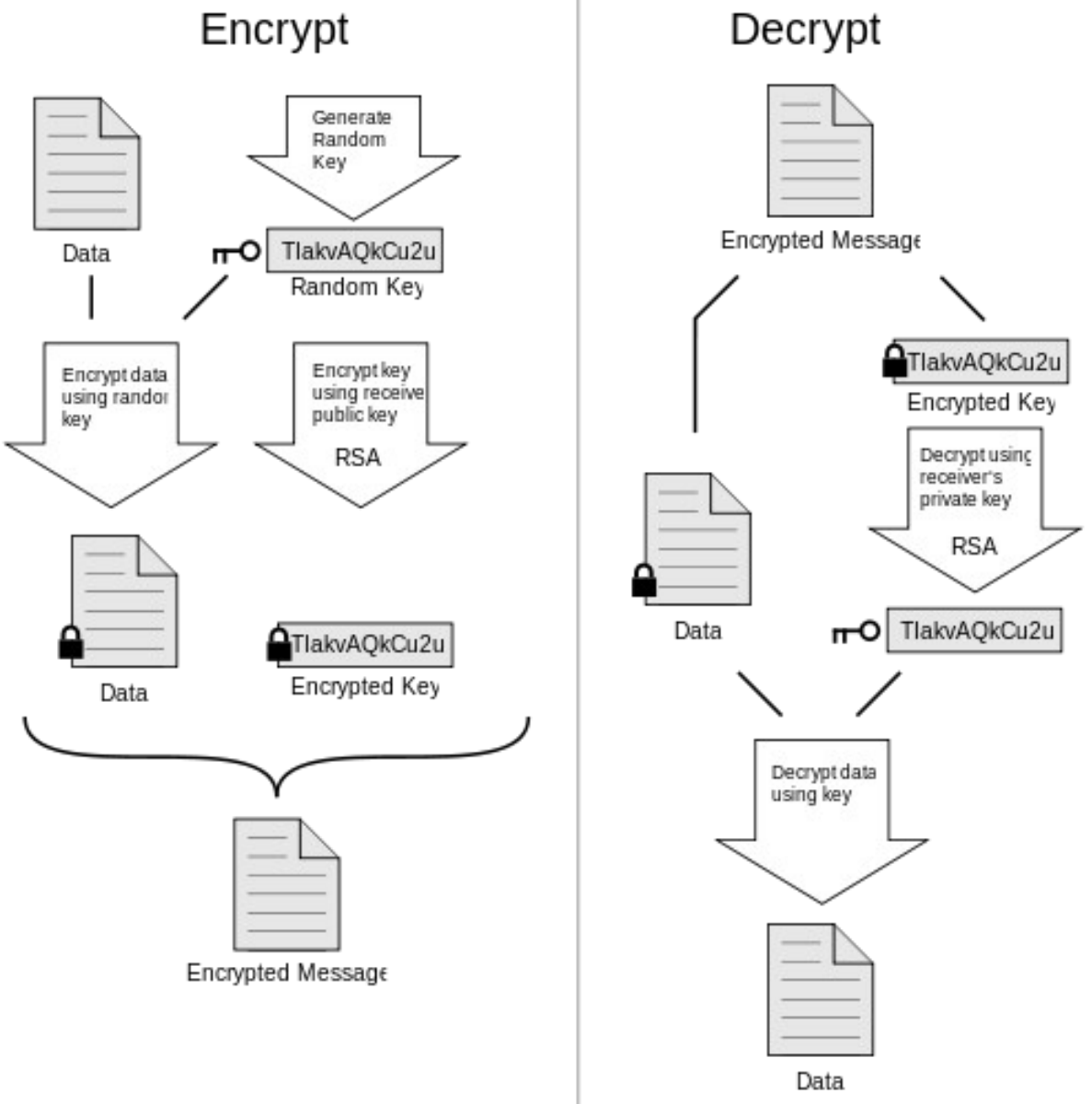
Overview

- Alice and Bod both create a pair of public and private keys.
- They both publish their public keys to the internet
- Alice fetches Bob's public key, encrypt a message, sends it over to Bob.
- Bob decrypts messages encrypted to his public key, using his private key
- Alice signs a message with her private key, sends message to Bob
- Bob verifies integrity and authenticity of message, as long as he has Alice's public key.

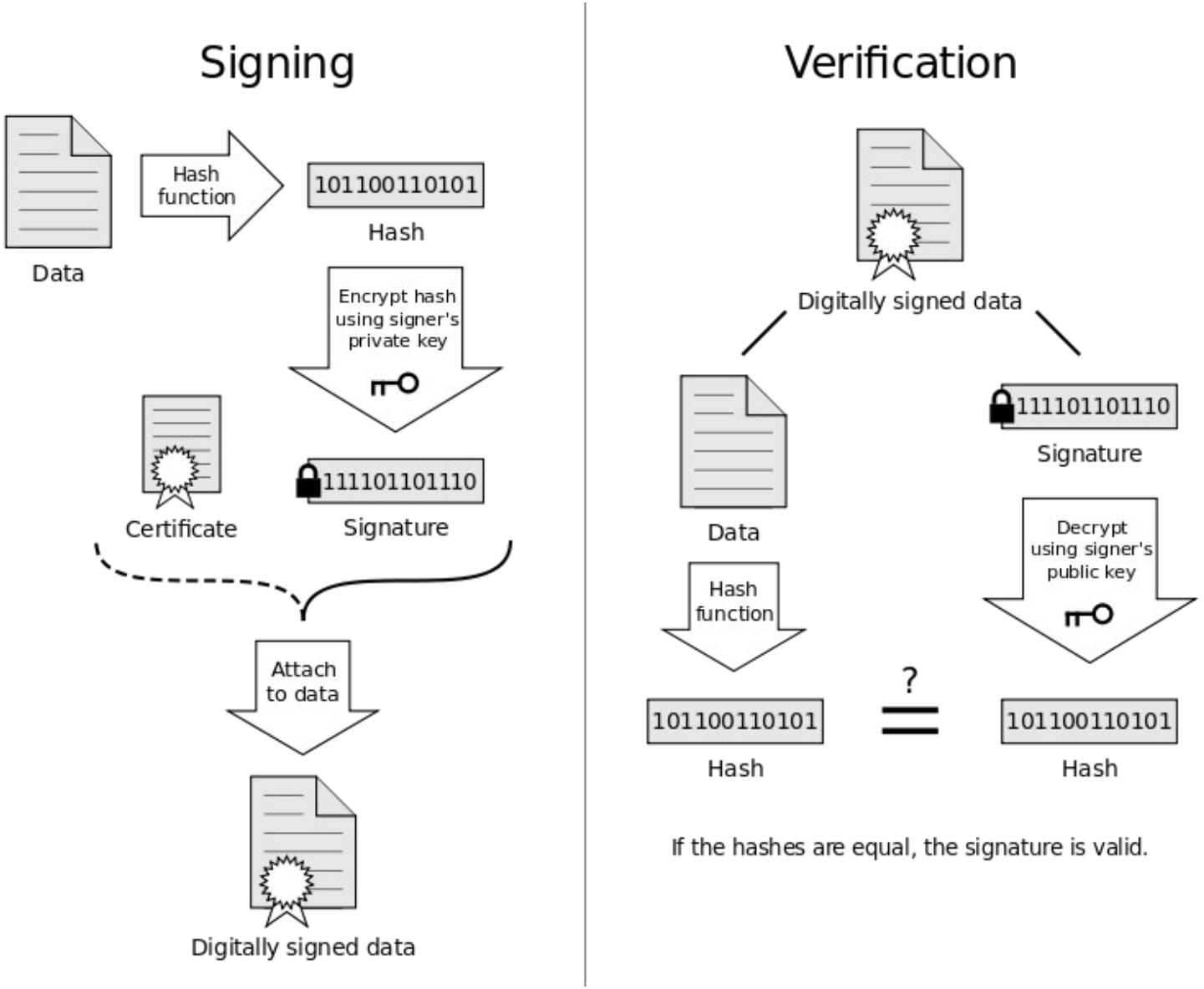
PGP, OpenPGP, GnuPG

- PGP είναι το πρόγραμμα που έφτιξε ο P.Zimmermann για ασφαλή επικοινωνία στα emails
- Χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας
- Data confidentiality, integrity, authenticity
- Το OpenPGP ειναι το ανοιχτό πρότυπο που προέκυψε απο το PGP
- Το GnuPG είναι η ελεύθερη υλοποίηση του προτύπου. Χρησιμοποιείται ευρέως σήμερα σε Linux και όχι μόνο σύστηματα

More Specifically (PGP)



Digital Signatures



Web of Trust

- How to bind public keys to identities?
- A central authority certifies all?
- WoT, in contrast to X.509 PKI, aims to be a distributed trust model
- If Bob has verified Alice's public key, can then sign it and publish this sig to the world.
- If Mallory wants to communicate with Alice, knows Bob's public key, trusts Bob's signatures, can then trust the Alice's key with Bob's signature.
- How to bootstrap? Organize key fingerprint verification meetings (they're not key signing parties)

Where is public key crypto used?

- TLS – Connection security, encryption + certification (HTTPS, IMAP, POP)
- SSH
- Crypto currencies
- OpenPGP, GnuPG
- ZRTP (voice)
- OTR – Off-the-record messaging
- TextSecure (read more about this)

How to use public key crypto?

- Encrypt and sign your emails, use Mozilla Thundebird + Enigmail plugin
- Get familiar with gpg tool in cli
- Verify every software you download
- Verify your linux distro image before installation
- Use Schleuder encrypted mailing list with your friends
- Digitally sign the software you distribute
- Digitally sign git commits

Gimme moar!

- https://en.wikipedia.org/wiki/Public-key_cryptography
- https://skytal.es/wiki/Public_Key_Crypto
- https://skytal.es/wiki/OpenPGP,_GnuPG,_PGP
- http://pgp.cs.uu.nl/ - Key trust paths
- https://www.void.gr/kargig/blog/2013/07/08/greek-pgp-web-of-trust-2012-edition/
- http://keys.mayfirst.org/
- https://help.riseup.net/en/security/message-security/openpgp/best-practices
- https://github.com/WhisperSystems/TextSecure/wiki/ProtocolV2
- https://github.com/OpenTechFund/secure-email
- http://schleuder2.nadir.org/
- https://wiki.debian.org/SecureApt