Εισαγωγή στην Κρυπτολογία 3

Ασφάλεια Τηλεπικοινωνιακών Συστημάτων
Κωδικός DIT114
Σταύρος ΝΙΚΟΛΟΠΟΥΛΟΣ

Ακεραιότητα

Μονόδρομη Κρυπτογράφηση

Ακεραιότητα

Αυθεντικότητα μηνύματος
Ακεραιότητα μηνύματος
Αυθεντικότητα / Ακεραιότητα Οντότητας

Συναρτήσεις Κατατεμαχισμού
Hash Functions

Κάνουν τη συμπίεση του Προκρούστη από αυθαίρετο σε σταθερό μέγεθος.

Μονόδρομη Κρυπτογράφηση – Hash Functions
Ιδιότητες ιδανικής συνάρτησης

- Είναι Αιτιοκρατικές – Το ίδιο ακριβώς μήνυμα παράγει ακριβώς την ίδια έξοδο.
- Είναι εύκολος και ταχύς ο υπολογισμός τους, ως προς την υλοποίηση
- Είναι πρακτικά αδύνατη η δημιουργία μηνύματος από μια έξοδο hash.
- Είναι πρακτικά αδύνατη η εύρεση δύο μηνυμάτων με την ίδια έξοδο hash.
- Μικρή αλλαγή σε ένα μήνυμα πρέπει να δημιουργεί τελείως διαφορετική έξοδο hash.

Ασφάλεια Τηλεπικοινωνιακών Διαύλων
(οι εισηγήσεις είναι τρίωρες ανά αριθμό)

1) Ασφάλεια Η/Υ ΕΙΣΑΓΩΓΗ

Εξοικείωση με τις έννοιες της Ασφάλειας σε Η/Υ και δίκτυα Η/Υ. Καθώς σήμερα μιλάμε για τηλεπικ
άπτεται στο σύνολο των τηλεπικοινωνιών. Ασφάλεια Χρηστών, προστασία προσωπικών δεδομένων,

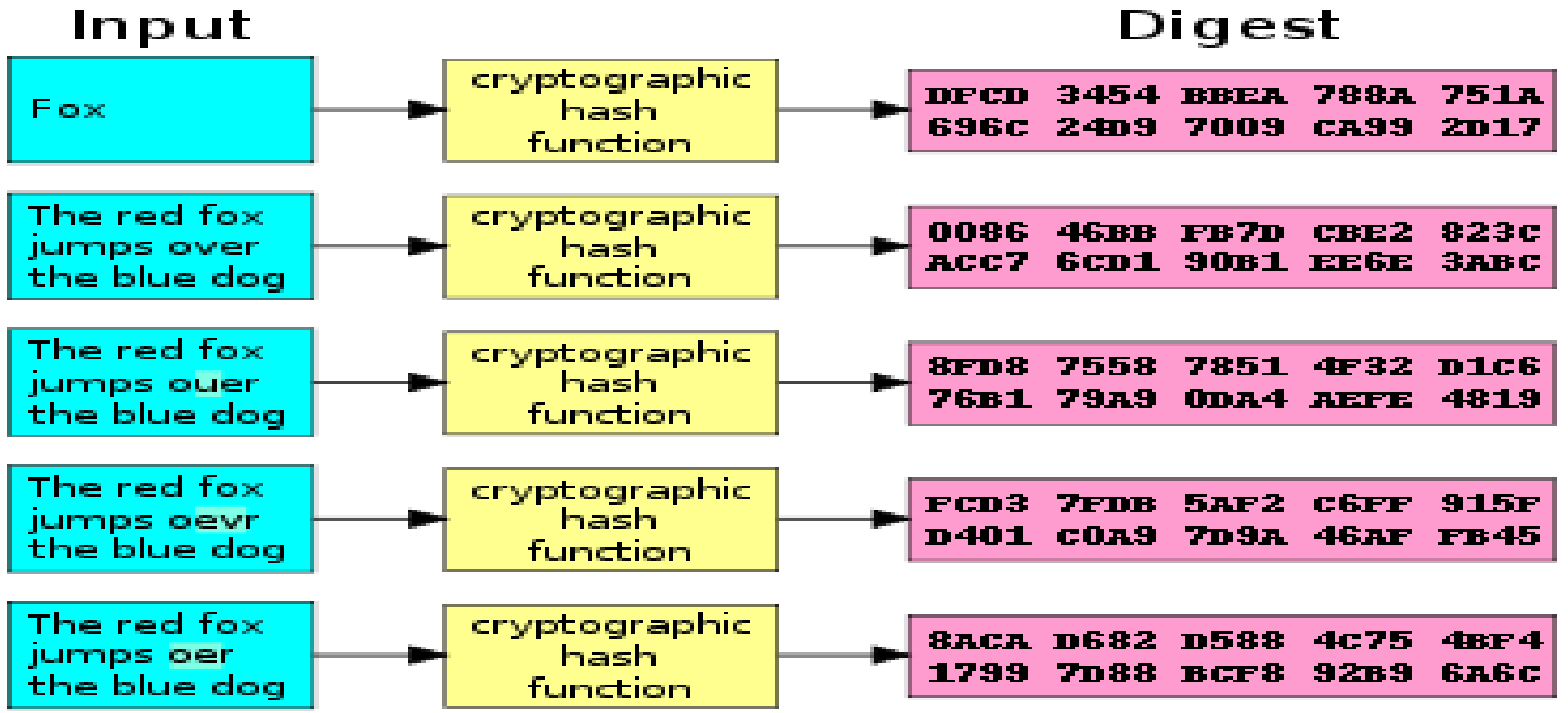
Ασφάλεια Τηλεπικοινωνιακών Διαύλων
(οι εισηγήσεις είναι δίωρες ανά αριθμό)

1) Ασφάλεια Η/Υ ΕΙΣΑΓΩΓΗ

Εξοικείωση με τις έννοιες της Ασφάλειας σε Η/Υ και δίκτυα Η/Υ. Καθώς σήμερα μιλάμε για τηλεπικ
άπτεται στο σύνολο των τηλεπικοινωνιών. Ασφάλεια Χρηστών, προστασία προσωπικών δεδομένων,

Filename	ÐáñÜäåéãìá 1 - Ýããñáöï word - ôñïðïðïéçìÝíï.docx
MD5	adb478bf384c907fe30e27f3b2dd31b9
SHA1	27f33e6f0fd02176e3fbef28d8e71f0819c76aa2
CRC32	97a55631
SHA-256	e98866159210a7e27668dcca098719b19fdc851f3e5451a1bc0f4f382e467827
SHA-512	762d0b693653ff7d566c262f639a5ac5c1563e40ea47cd0fbaf891fcf21976739c00898c13d38c7f35950c1dc7aa8ab23eeb3c6dc84773ddcdcc953a4e97055c
SHA-384	1dac077e2097866256fccb5f9c7fa00450174801fb5d849c2a47cff71bde8d88a3d4868014665f8f659c817c35ec46a4

Filename	ÐáñÜäåéãìá 1 - Ýããñáöï word.docx
MD5	df66b316b8f164c12e21883dd6604123
SHA1	f8dcf399279d0114b2cf78f37b7dd25039fd37b7
CRC32	08e21f7b
SHA-256	e98a3721f54545dbd889990b24dd12a5765986ebf3f7adbbb5c4af34047c07cc
SHA-512	cd97e0c2c01d1d30bae40a107ee1fd3168cd49a2b0d79dcfeeacd38c6a7476a1bed3061a992f84256c269eaeef387a7ac3b4015a25976ed18297f0732c7470e2
SHA-384	6066b7be8e3d3f807f3505665532192d4d3bf3ef2e4450db470b73a399d36424f62ffb76c321484be0a9d3f53bffc196



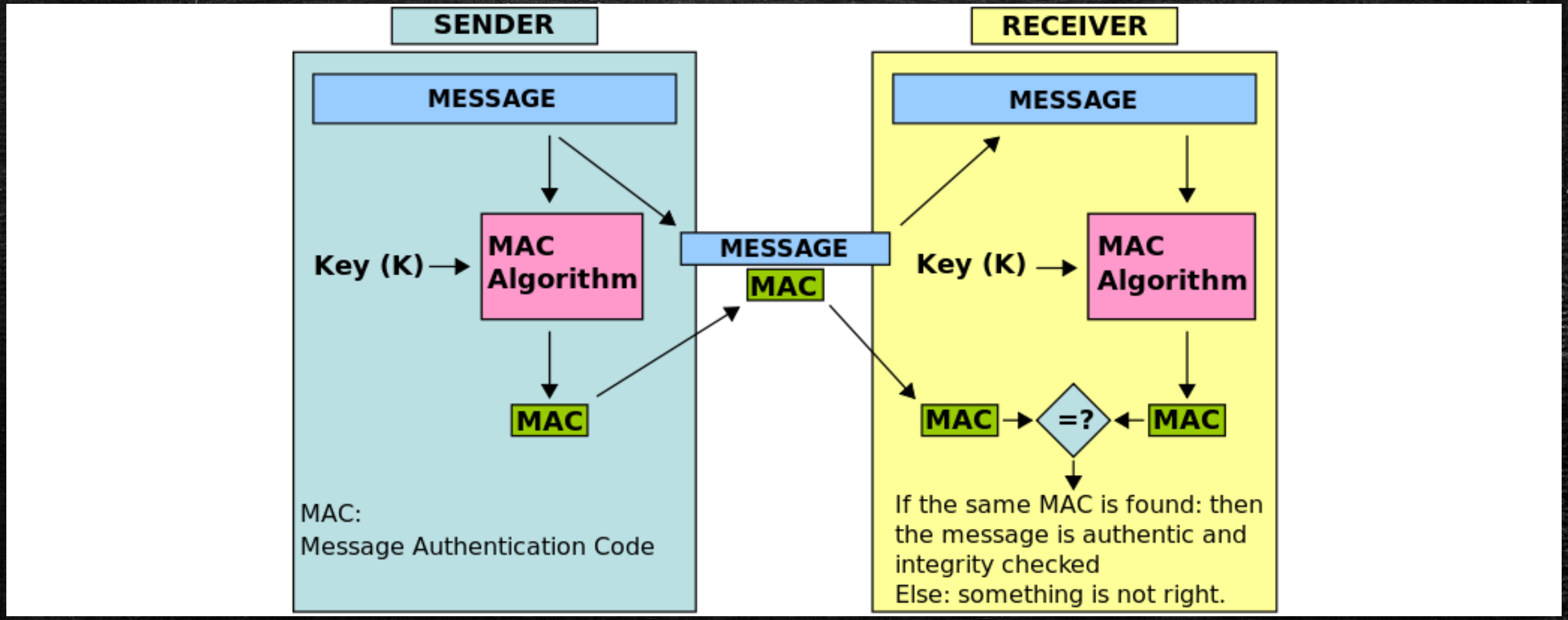
A cryptographic hash function (specifically SHA-1) at work. A small change in the input (in the word "over") drastically changes the output (digest). This is the so-called avalanche effect.

V·T·E	Cryptographic hash functions & message authentication codes
	List · Comparison · Known attacks
Common functions	MD5 · SHA-1 · SHA-2 · SHA-3 · BLAKE2
SHA-3 finalists	BLAKE · Grøstl · JH · Skein · Keccak (winner)
Other functions	CubeHash · ECOH · FSB · GOST · HAS-160 · HAVAL · Kupyna · LM hash · MD2 · MD4 · MD6 · MDC-2 · N-Hash · RIPEMD · RadioGatún · SWIFFT · Snefru · Streebog · Tiger · VSH · Whirlpool
Key derivation functions	bcrypt · crypt · PBKDF2 · scrypt · Argon2
MAC functions	DAA · CBC-MAC · HMAC · OMAC/CMAC · PMAC · VMAC · UMAC · Poly1305 · SipHash
Authenticated encryption modes	CCM · CWC · EAX · GCM · IAPM · OCB
Attacks	Collision attack · Preimage attack · Birthday attack · Brute-force attack · Rainbow table · Side-channel attack · Length extension attack
Design	Avalanche effect · Hash collision · Merkle–Damgård construction · Sponge function · HAIFA construction · Unique Block Iteration
Standardization	CRYPTREC · NESSIE · NIST hash function competition
Utilization	Hash-based cryptography · Key stretching · Merkle tree · Message authentication · Proof of work · Salt

Εφαρμογές Συναρτήσεων κατατεμαχισμού

- Επαλήθευση της ακεραιότητας μηνύματος
- Επαλήθευση κωδικού (password)
- Σήμανση εργασίας
- Σήμανση και αναγνώριση Αρχείων
- Γεννήτρια ψευδοτυχαίων αριθμών
- Γεννήτρια κωδικών (passwords)

Κώδικες Αυθεντικότητας Μηνύματος
Message Authentication codes (MACs)



Hash-based message authentication code

This definition is taken from RFC 2104:

$$\mathrm{HMAC}(K, m) = H\Big((K' \oplus opad) \,||\, H\big((K' \oplus ipad) \,||\, m\big)\Big)$$

MAC / MIC etc. Ποιο πρόβλημα υπάρχει?

- Η ανάγκη να έχουν και ο Αποστολέας και ο Παραλήπτης την ίδια κλείδα k.
- Είναι το ίδιο πρόβλημα όπως με τη συμμετρική κρυπτογράφηση.
- Η κλείδα k μπορεί να παράγεται από έναν αλγόριθμο.
- Πρέπει όμως να είναι μοναδική και για τους δύο και να χρησιμοποιηθεί μόνο μια φορά.
- Πρέπει να εμπεριέχει την ιδέα του χρόνου.

Αυθεντικοποίηση Χρήστη

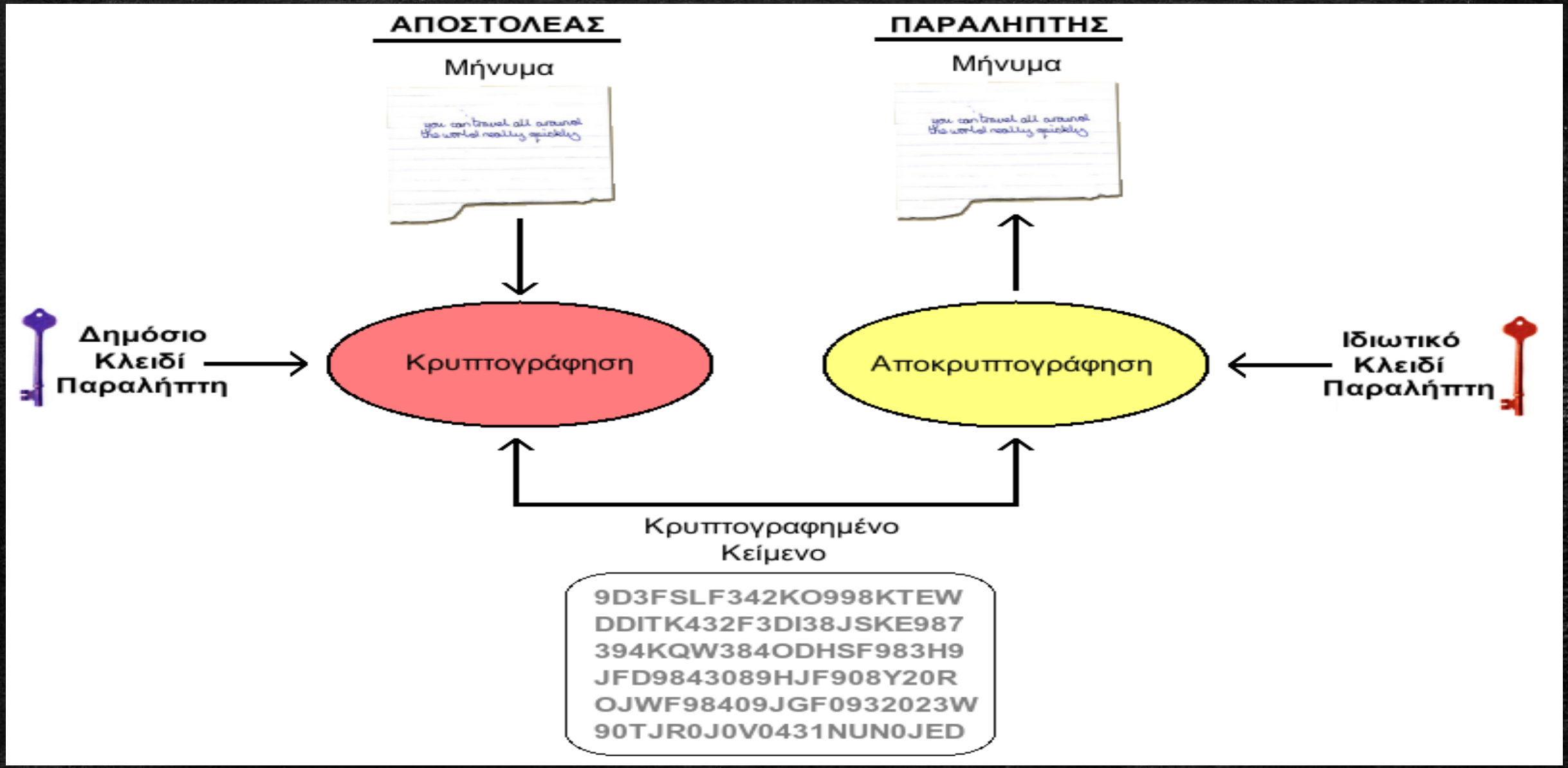
Ασύμμετρη Κρυπτογραφία

Κρυπτογράφηση Δημόσιου Κλειδιού

- Προσθέστε την πρώτη κουκκίδα εδώ
- Προσθέστε τη δεύτερη κουκκίδα εδώ
- Προσθέστε την τρίτη κουκκίδα εδώ

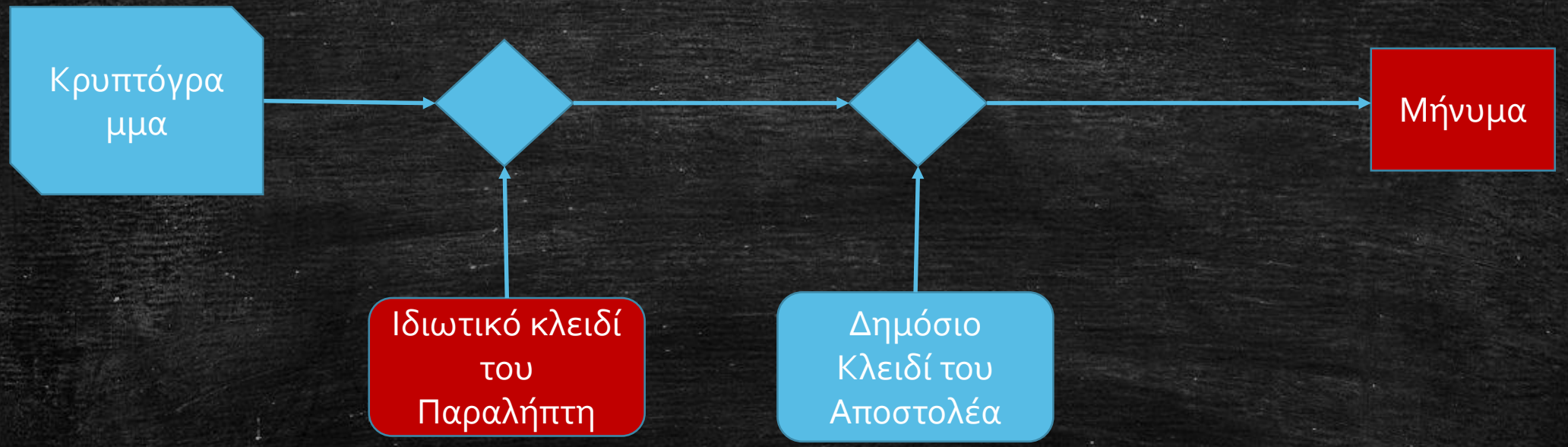
ΠΙΣΤΟΠΟΙΗΣΗ ΑΠΟΣΤΟΛΕΑ

ΠΙΣΤΟΠΟΙΗΣΗ ΠΑΡΑΛΗΠΤΗ



ΠΙΣΤΟΠΟΙΗΣΗ ΠΑΡΑΛΗΠΤΗ - ΑΠΟΣΤΟΛΕΑ

ΠΙΣΤΟΠΟΙΗΣΗ ΠΑΡΑΛΗΠΤΗ - ΑΠΟΣΤΟΛΕΑ



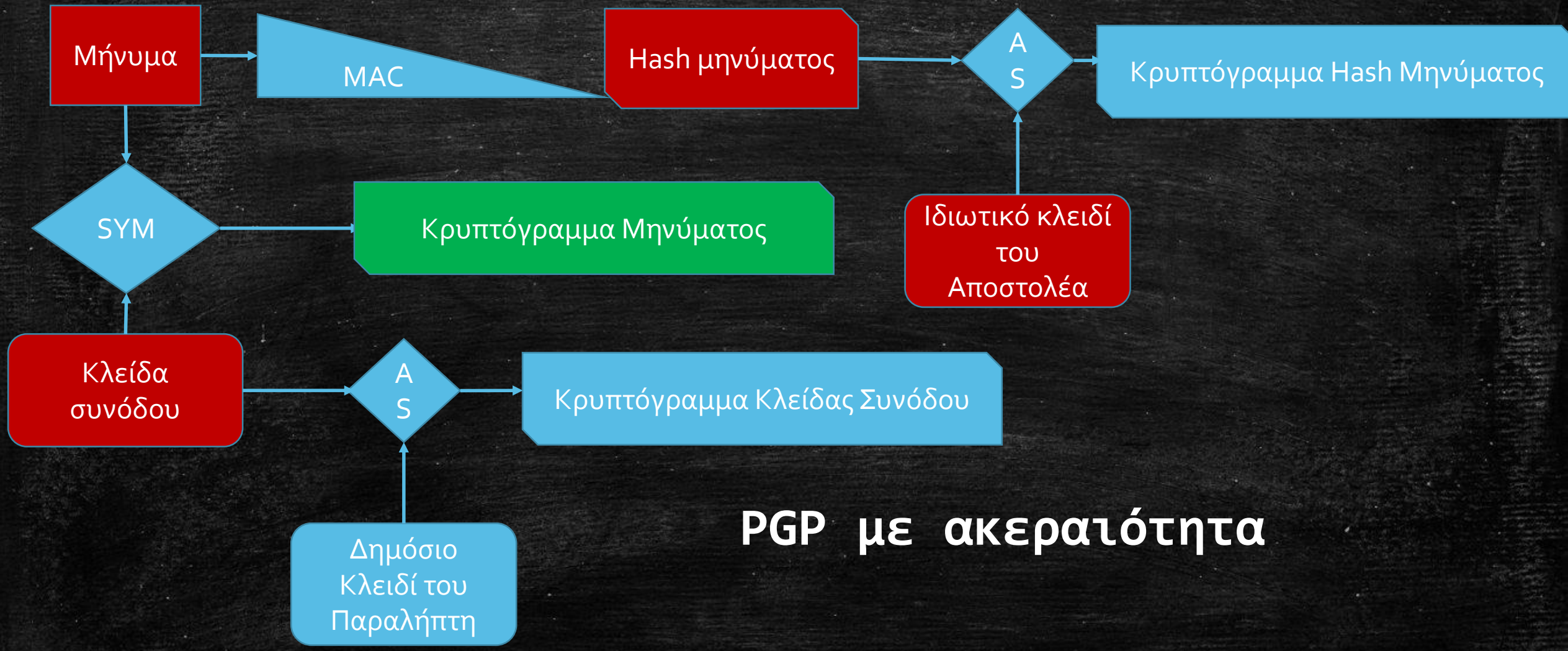
Παραδείγματα:

- Πρωτόκολλο ανταλλαγής κλείδας Diffy-Hellman
- Στάνταρ ψηφιακών υπογραφών
- ElGamal.
- Τεχνικές ελλειπτικών καμπύλων
- Διάφορες τεχνικές συμφωνίας κλείδας συνόδου
- Κρυπτοσύστημα Paillier.
- RSA
- Κρυπτοσύστημα Cramer-Shoup
- Πρωτόκολλο συμφωνίας κλείδας συνόδου YAK

Προβλήματα Κρυπτογράφησης Δημόσιου Κλειδιού

- Ύπαρξη Τρίτης Έμπιστης Οντότητας που θα διανείμει τα ζευγάρια των κλειδών, και θα εγγυάται την εγκυρότητά τους. Certification Authority.
- Ύπαρξη Έμπιστου καταλόγου.
- Διανομή των ζευγαριών των κλειδών.
- Το μήνυμα πρέπει να είναι μικρότερο της κλείδας. .

ΣΥΝΔΥΑΣΜΟΣ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ – ΑΚΕΡΑΙΟΤΗΤΑΣ - ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ



PGP με ακεραιότητα

ΠΛΕΥΡΑ ΤΟΥ ΑΠΟΣΤΟΛΕΑ

Δημόσιο Κλειδί του Παραλήπτη

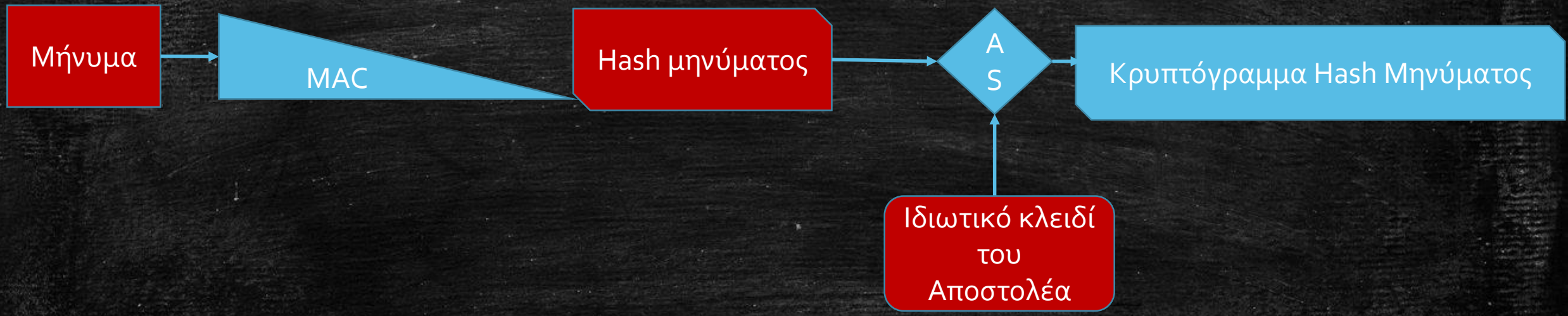
Ιδιωτικό κλειδί του Αποστολέα

Μήνυμα

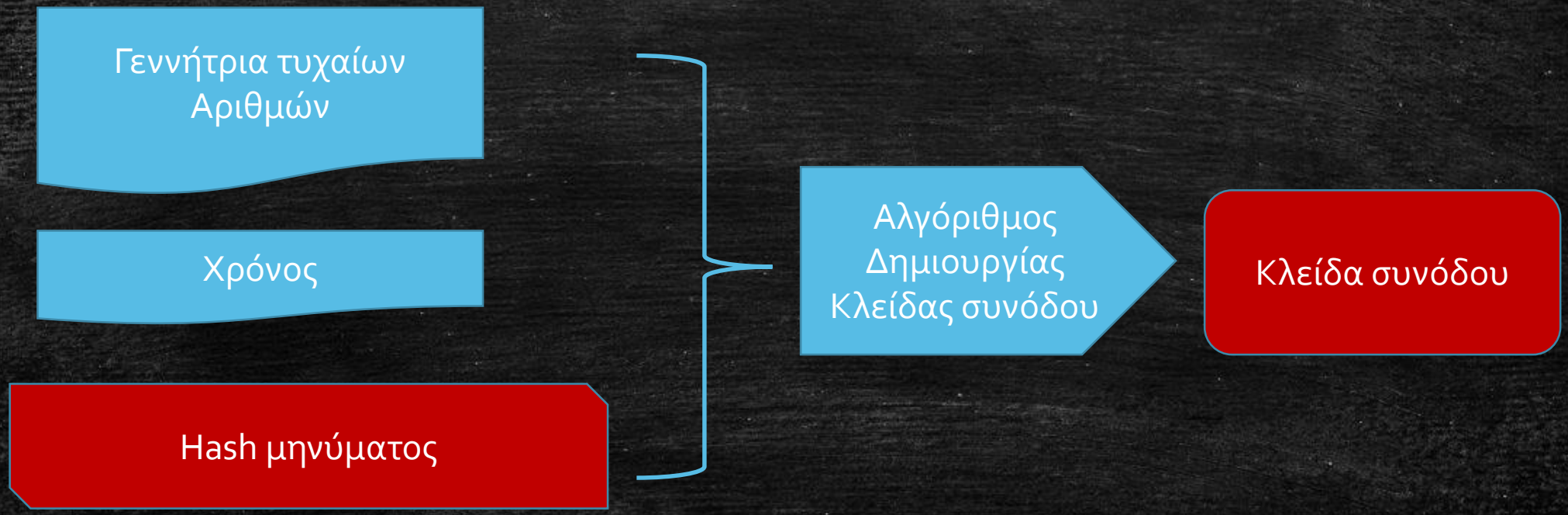
Κλείδα συνόδου

?

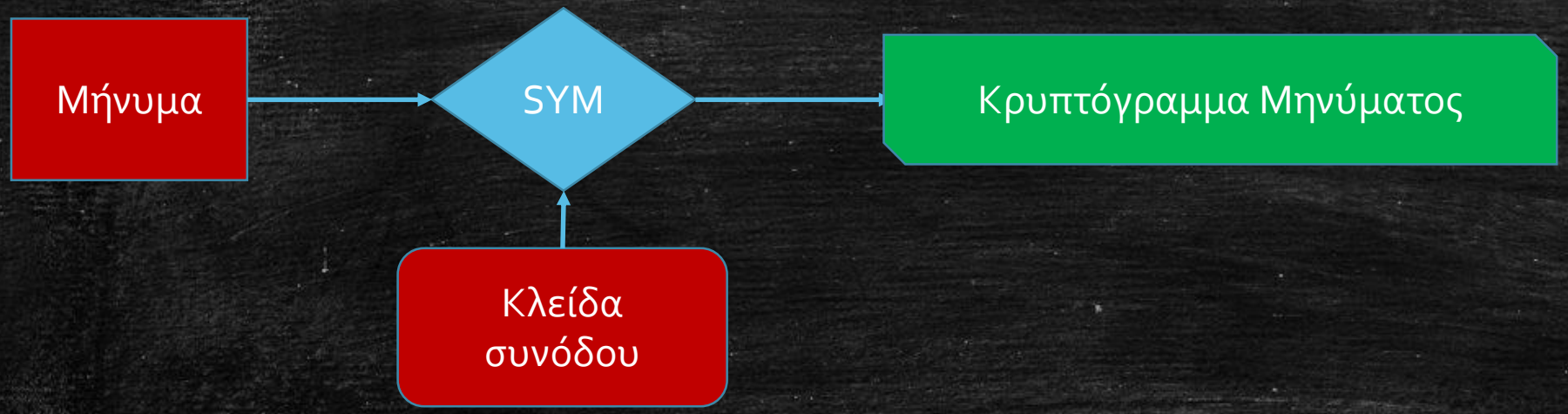
ΔΙΑΔΙΚΑΣΙΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΑΠΟΣΤΟΛΕΑ



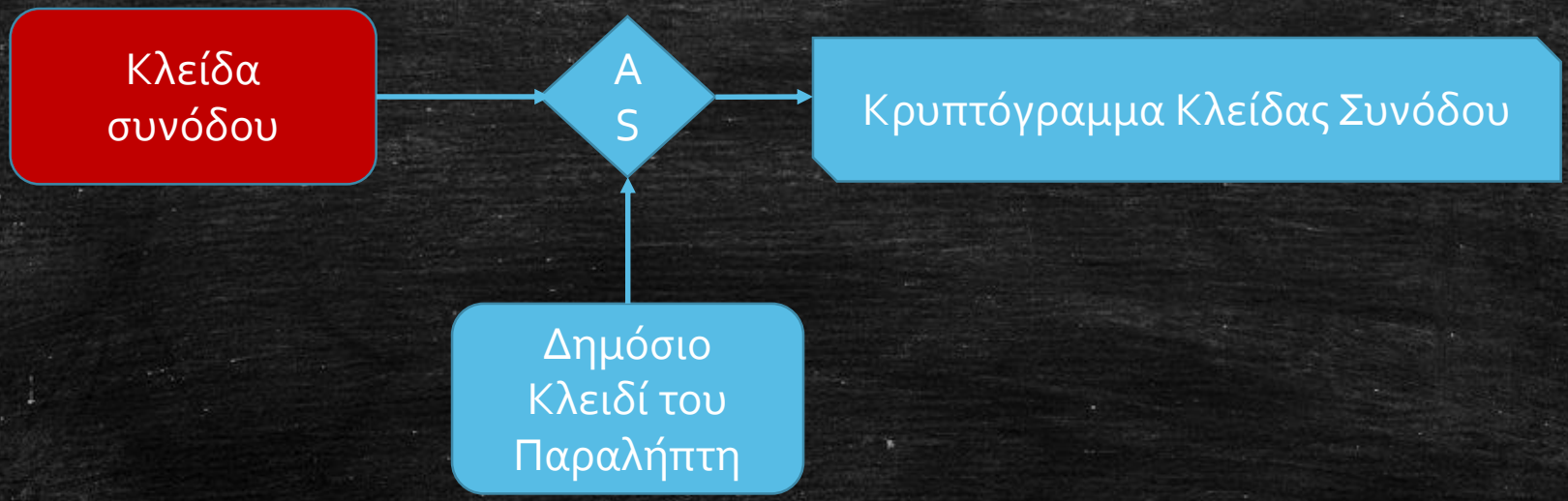
ΔΗΜΙΟΥΡΓΙΑ ΚΛΕΙΔΑΣ ΣΥΝΟΔΟΥ



ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΜΗΝΥΜΑΤΟΣ



ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΛΕΙΔΑΣ ΣΥΝΟΔΟΥ



ΣΥΝΕΝΩΣΗ ΤΩΝ ΚΡΥΠΤΟΓΡΑΜΜΑΤΩΝ

ΠΡΟΣΟΧΗ: η σειρά ένωσης παίζει ρόλο

ΠΛΕΥΡΑ ΤΟΥ ΠΑΡΑΛΗΠΤΗ – ΕΞΑΓΩΓΗ ΚΛΕΙΔΩΝ

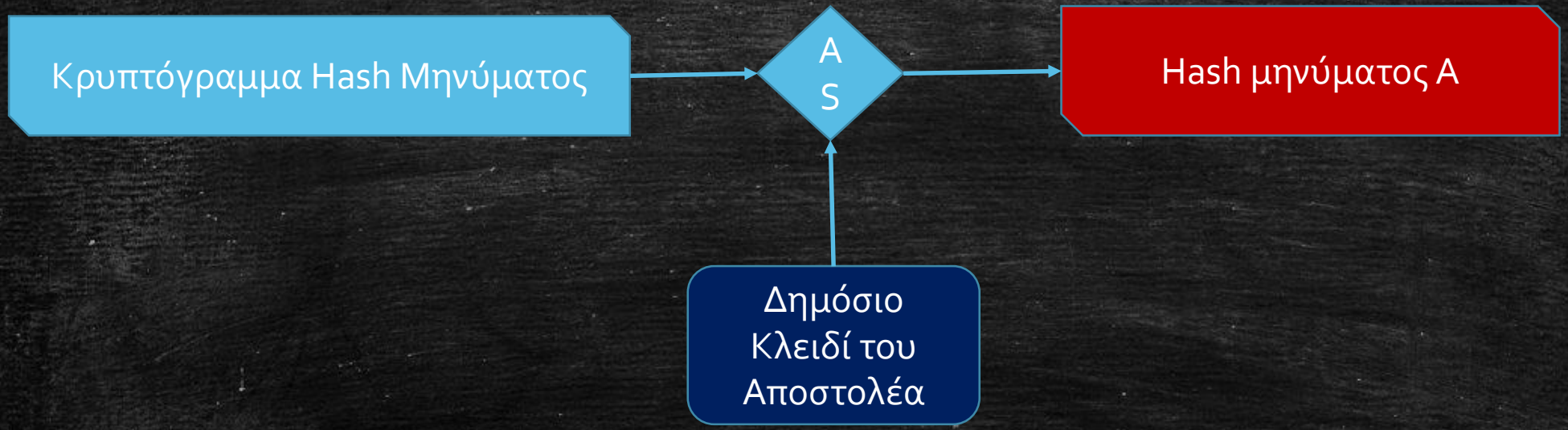
Τελικό Κρυπτόγραμμα

- Κρυπτόγραμμα Hash Μηνύματος
- Κρυπτόγραμμα Κλείδας Συνόδου
- Κρυπτόγραμμα Μηνύματος

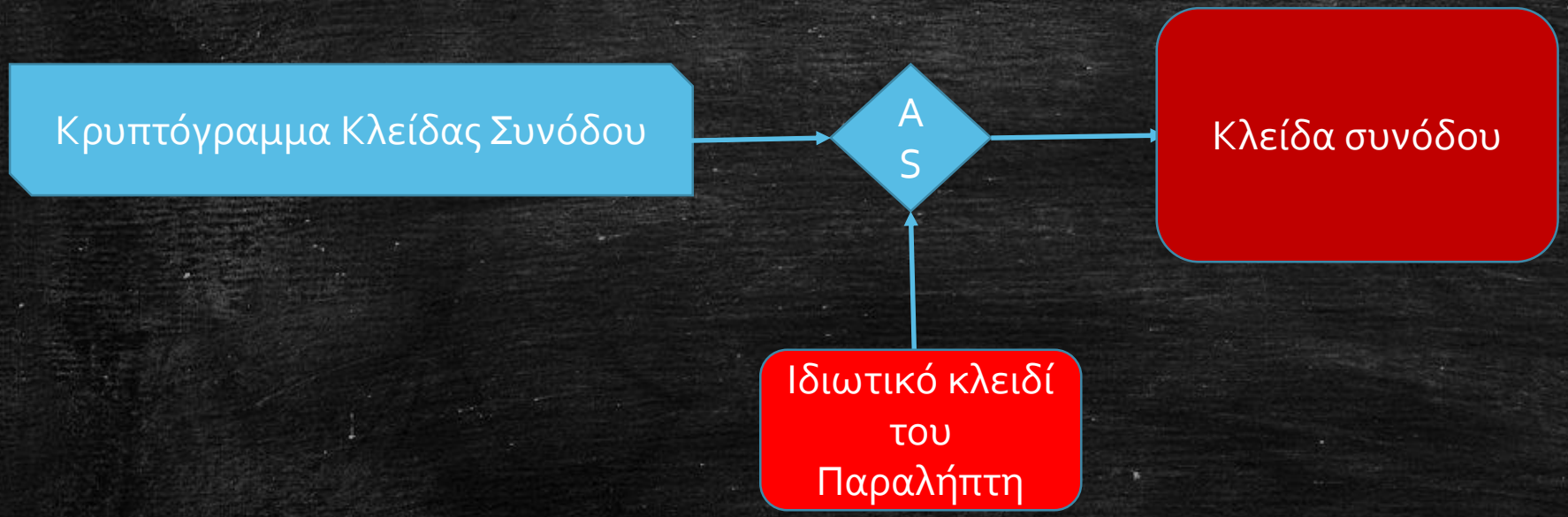
Δημόσιο Κλειδί του Αποστολέα

Ιδιωτικό κλειδί του Παραλήπτη

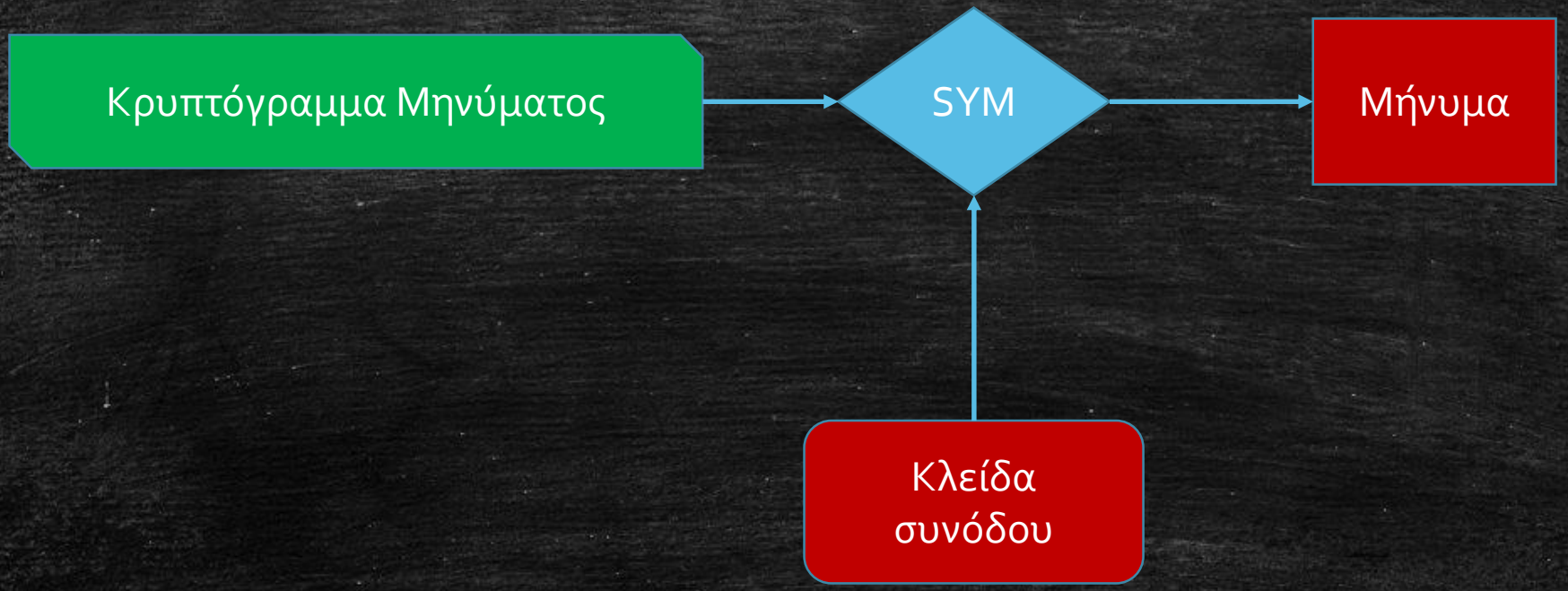
ΕΞΑΓΩΓΗ HASH ΜΗΝΥΜΑΤΟΣ



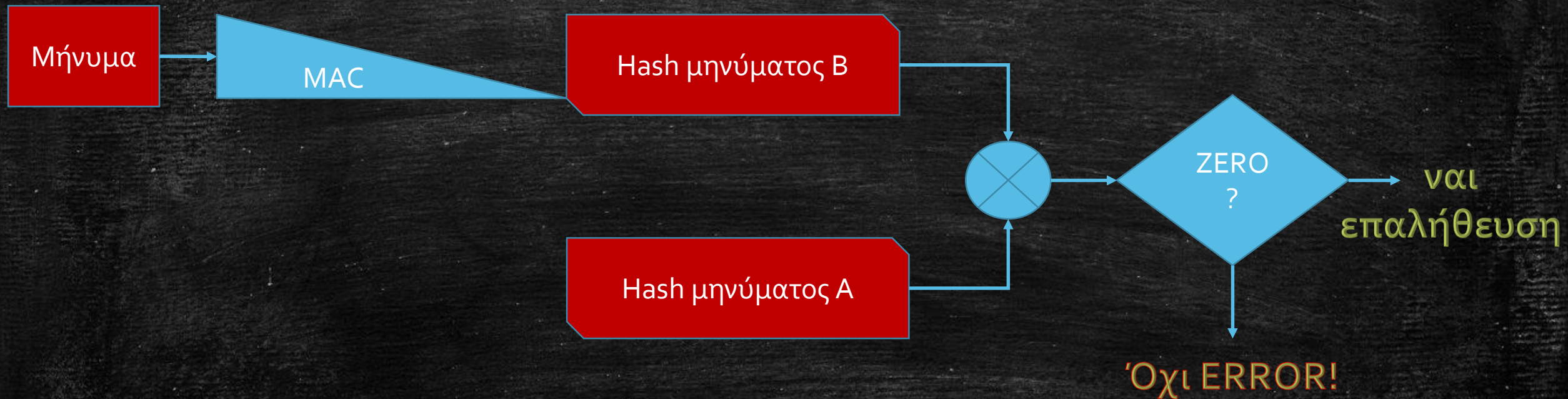
ΕΞΑΓΩΓΗ ΚΛΕΙΔΑΣ ΣΥΝΟΔΟΥ



ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ ΜΗΝΥΜΑΤΟΣ



ΕΠΑΛΗΘΕΥΣΗ ΜΗΝΥΜΑΤΟΣ



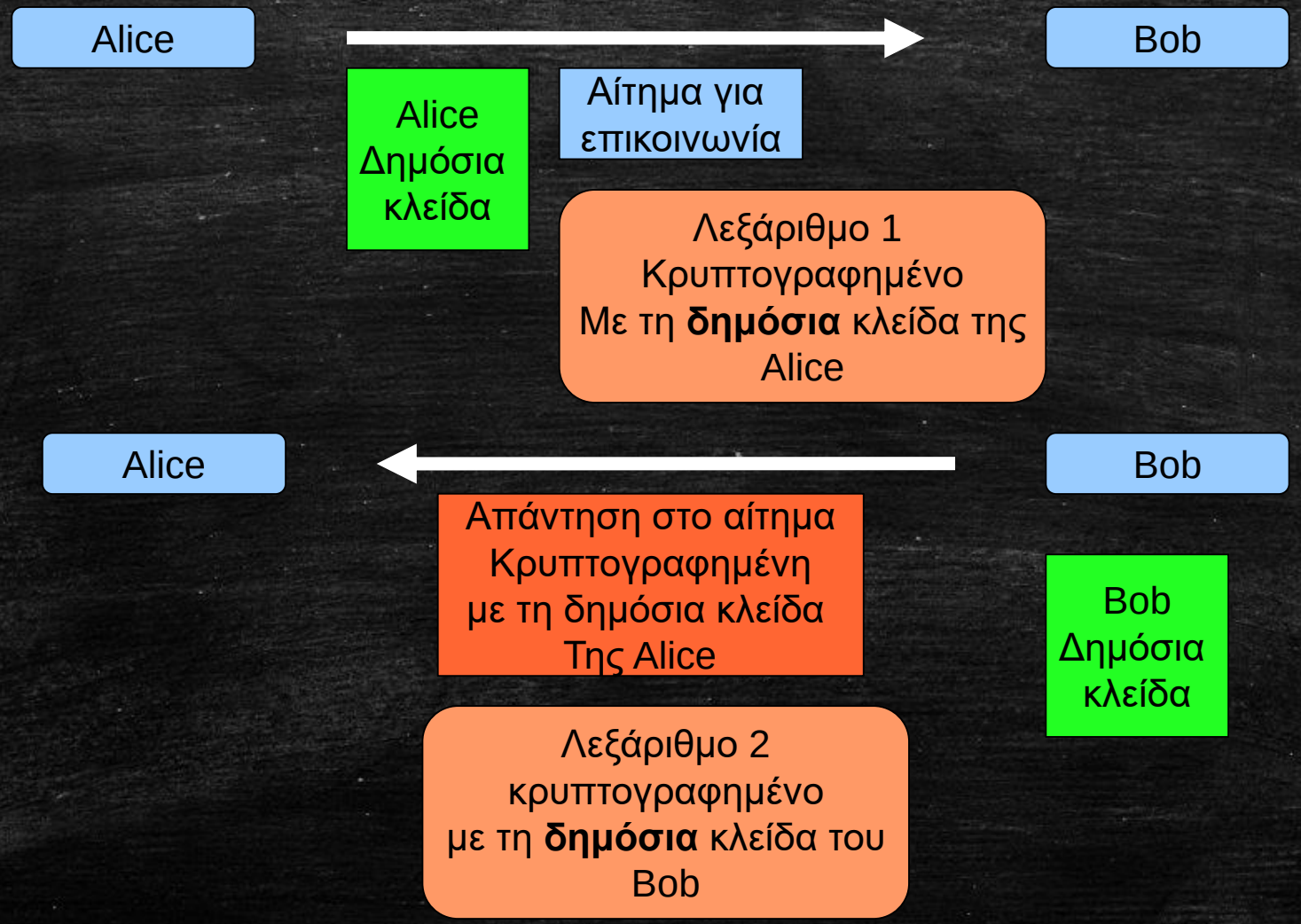
Κρυπτογραφικά πρωτόκολλα

Ένα κρυπτογραφικό πρωτόκολλο καλείται να εγκαθιδρύσει μια ασφαλή επικοινωνία μεταξύ δύο πλευρών (συνδρομητών).

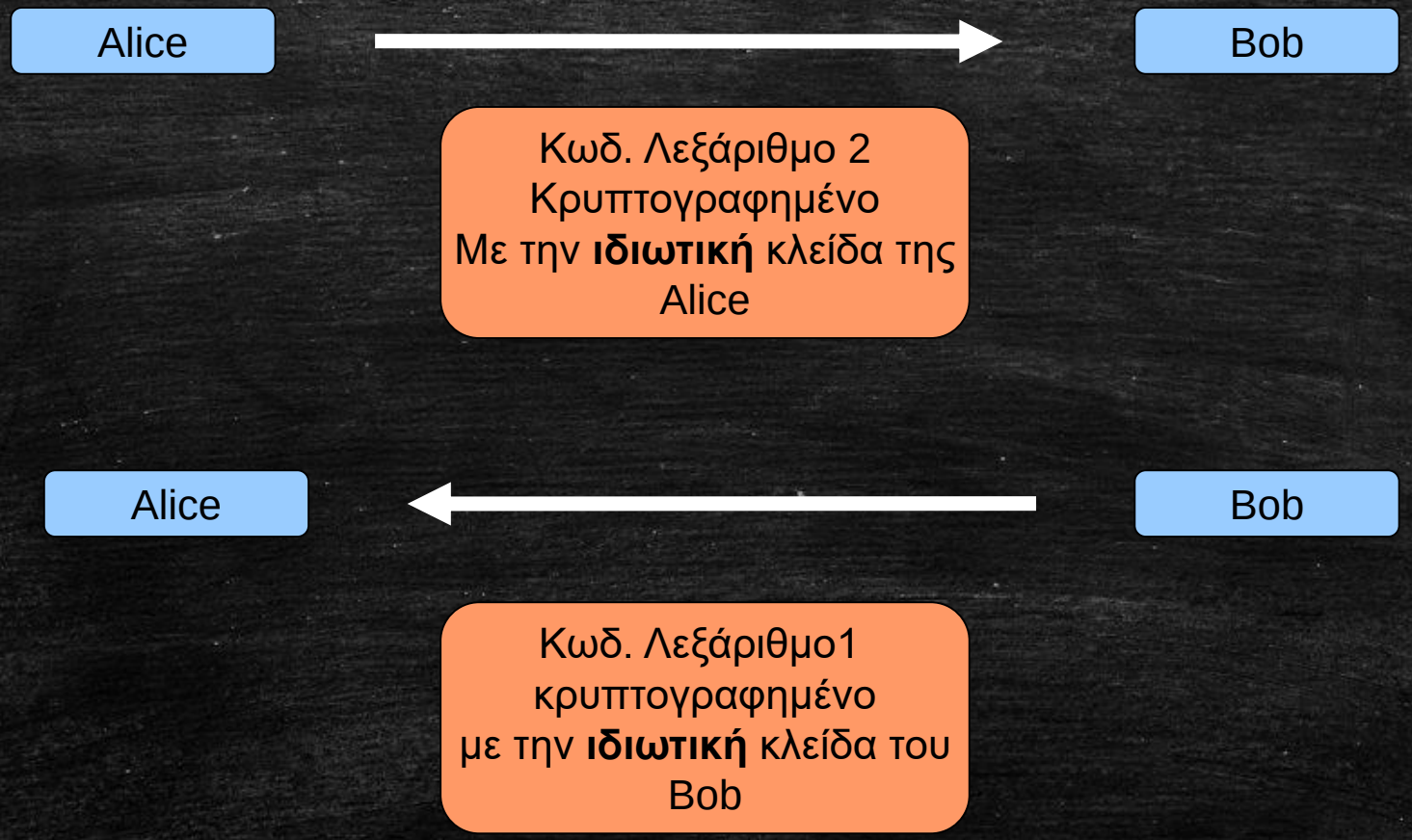
Μια ασφαλής επικοινωνία, όπως γνωρίζουμε εμπεριέχει:

Εμπιστευτικότητα **(Confidentiality)**
Ακεραιότητα **(Integrity)**
Διαθεσιμότητα **(Availability)**
Αυθεντικοποίηση (Aythentication)
Μη αποποίηση (Non Repudiation)

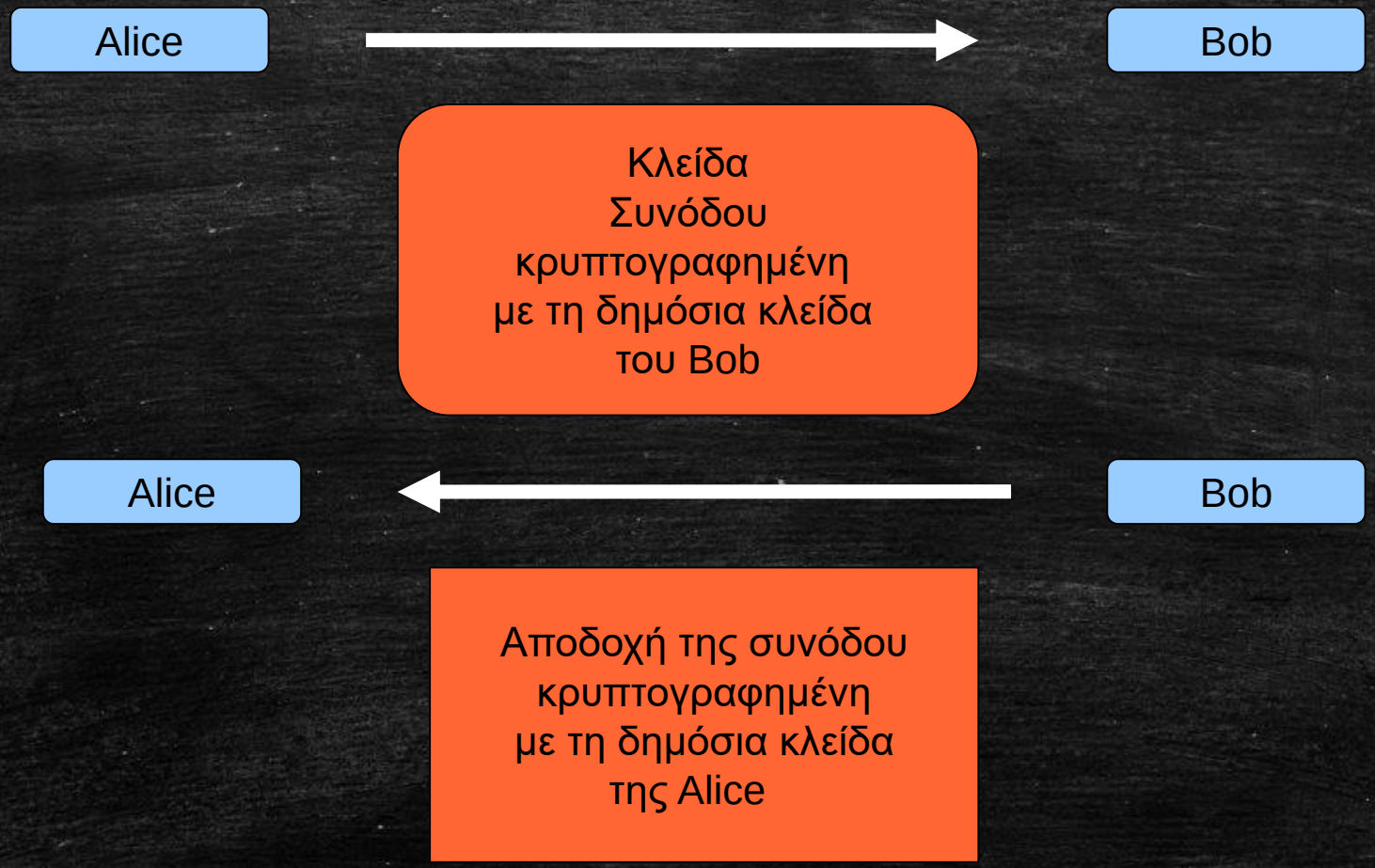
ΠΑΡΑΔΕΙΓΜΑ
Εγκαθίδρυσης Κλείδας Συνόδου



ΠΑΡΑΔΕΙΓΜΑ
Ασφαλούς επικοινωνίας



ΠΑΡΑΔΕΙΓΜΑ
Ασφαλούς επικοινωνίας



Ασφαλής επικοινωνία

Επαλήθευση της δυνατότητας συνόδου, με ανταλλαγή μηνυμάτων κρυπτογραφημένων με την κλείδα συνόδου

Κρυπτογραφικό πρωτόκολλο

Ένα κρυπτογραφικό πρωτόκολλο συνήθως υλοποιεί κάποιες από τις παρακάτω λειτουργίες:

- Συμφωνία ή εγκαθίδρυση κλείδας συνόδου
- Αυθεντικοποίηση ταυτότητας.
- Συμμετρική κρυπτογράφηση και υλοποίηση ακεραιότητας μηνύματος
- Ασφαλή διαβίβαση των δεδομένων, ανάλογα με το επίπεδο επικοινωνίας
- Μεθόδους μη αποποίησης
- Μεθόδους ανταλλαγής εμπιστευτικών δεδομένων
- Ασφαλή επικοινωνία ομάδας

Κρυπτογραφικά πρωτόκολλα

Internet Key Exchange
Ipsec
Kerberos
Off the record messaging
Point 2 Point Protocol
Signal Protocol
Transport Layer Security (TLS)
composed of Z and Real-time Transport Protocol (ZRTP)

Alice

Δημόσιο
Δίκτυο

Bob

Πρωτόκολλο εγκαθίδρυσης κι ανταλλαγής κλείδας Diffie-Hellman

Alice

Bob

p, q

a

$A = q^a \bmod p$

$B = q^b \bmod p$

b

$S = B^a \bmod p$

$R = A^b \bmod p$

$S = B^a \bmod p \equiv R = A^b \bmod p$

Πρωτόκολλο εγκαθίδρυσης κι ανταλλαγής κλείδας Diffie-Hellman

Alice		Bob		Eve	
Known	Unknown	Known	Unknown	Known	Unknown
$p = 23$		$p = 23$		$p = 23$	
$g = 5$		$g = 5$		$g = 5$	
$a = 6$	b	$b = 15$	a		a, b
$A = 5^a \bmod 23$		$B = 5^b \bmod 23$			
$A = 5^6 \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$			
$B = 19$		$A = 8$		$A = 8$, $B = 19$	
$s = B^a \bmod 23$		$s = A^b \bmod 23$			
$s = 19^6 \bmod 23 = 2$		$s = 8^{15} \bmod 23 = 2$			s

Πρωτόκολλο εγκαθίδρυσης κι ανταλλαγής κλείδας Diffie-Hellman

- Το πρωτόκολλο Diffie-Hellman είναι το πρώτο παράδειγμα πρωτοκόλλου εγκαθίδρυσης κι ανταλλαγής κλείδας.
- Προσοχή, δεν παρέχει αυθεντικοποίηση
  - Ούτε η Alice ούτε ο Bob γνωρίζουν επακριβώς με ποιόν αντάλλαξαν κλείδες.
  - Επομένως χωρίς αυθεντικοποίηση, δεν μπορεί ούτε η εμπιστευτικότητα να πιστοποιηθεί
- Εντούτοις μαζί με αυθεντικοποίηση έχει πολλά πλεονεκτήματα καθώς εμπεριέχει την ιδιότητα της PFS (Perfect Forward Secrecy). Μια αποκάλυψη μελλοντικής κλείδας δεν αποκαλύπτει προηγούμενες επικοινωνίες.

Πρωτόκολλο εγκαθίδρυσης κι ανταλλαγής κλείδας Needham - Schroeder

$K_{A,TTP}$

Alice

Trusted Third Party
TTP

$K_{B,TTP}$

Bob

r_A →

$\{A, B, r_A\}$

$\{K_{A,B}, A\}_{K_{B,TTP}}$

Κλείδα συνόδου $K_{A,B}$

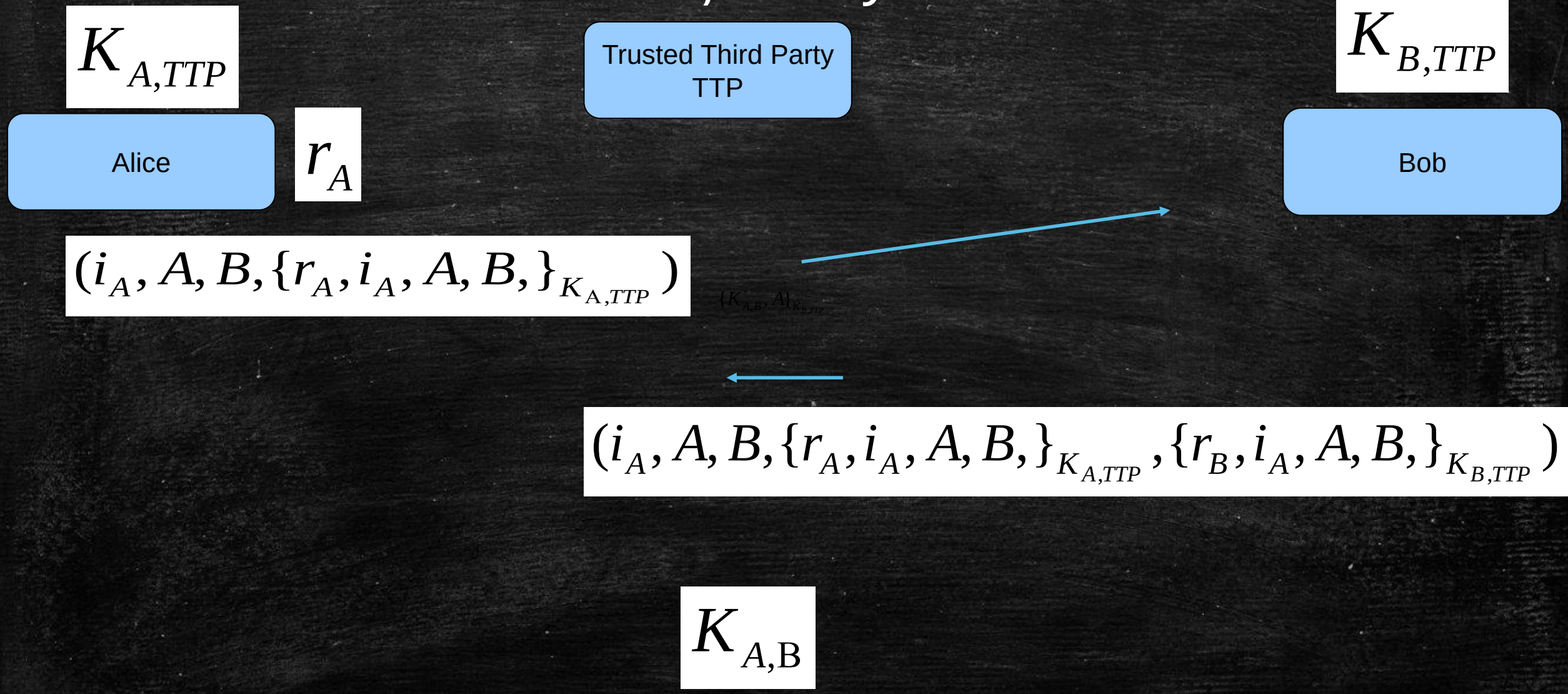
←

$\{r_A, B, K_{A,B}, \{K_{A,B}, A\}_{K_{B,TTP}}\}_{K_{A,TTP}}$

$\{K_{A,B}, A\}_{K_{B,TTP}}$ →

Πρωτόκολλο εγκαθίδρυσης κι ανταλλαγής κλείδας Needham – Schroeder (συνέχεια)

Πρωτόκολλο εγκαθίδρυσης κι ανταλλαγής κλείδας Otway-Rees



Πρωτόκολλο εγκαθίδρυσης κι ανταλλαγής κλείδας Otway-Rees (συνέχεια)

Trusted Third Party
TTP

$K_{A,B}$

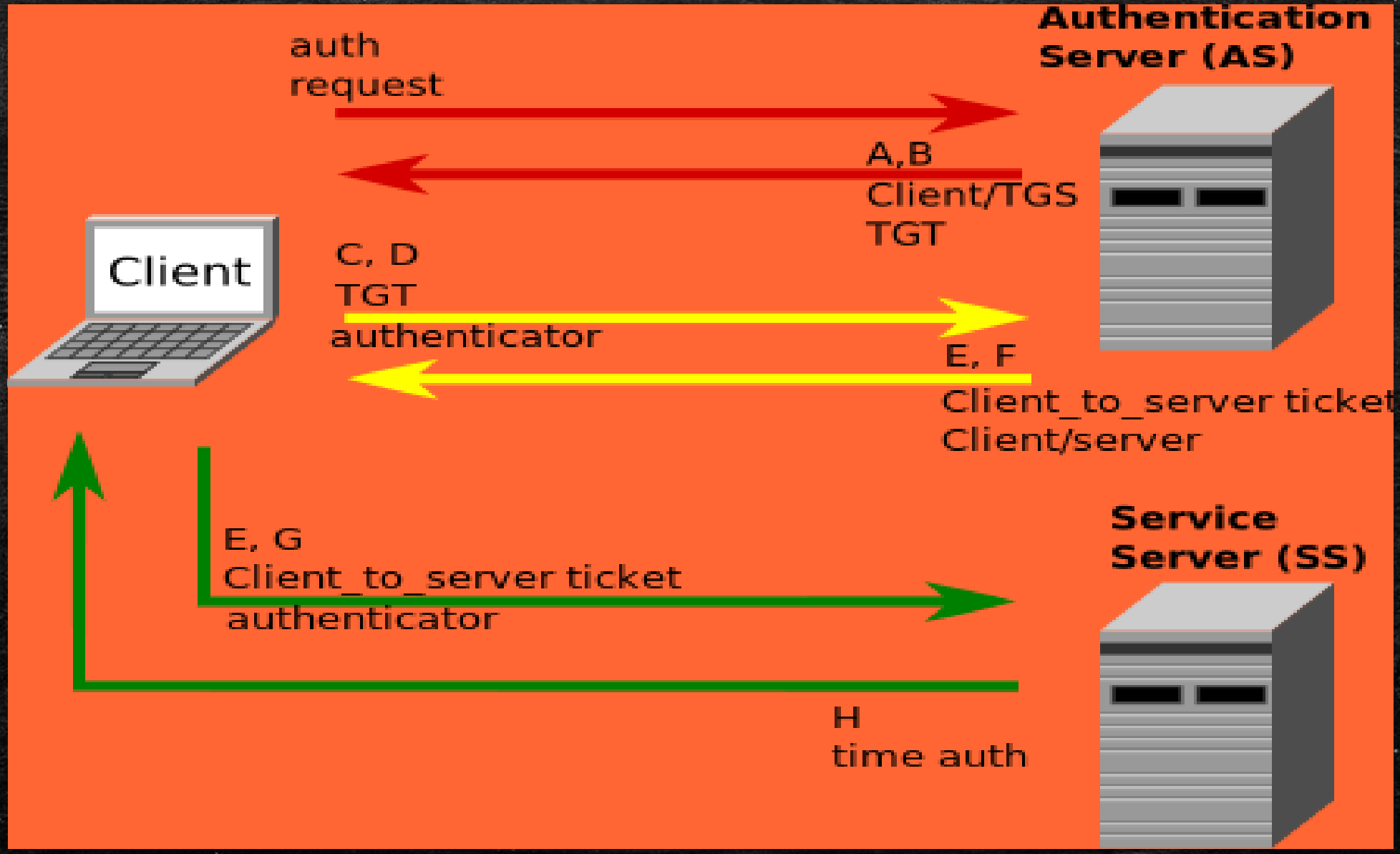
Alice

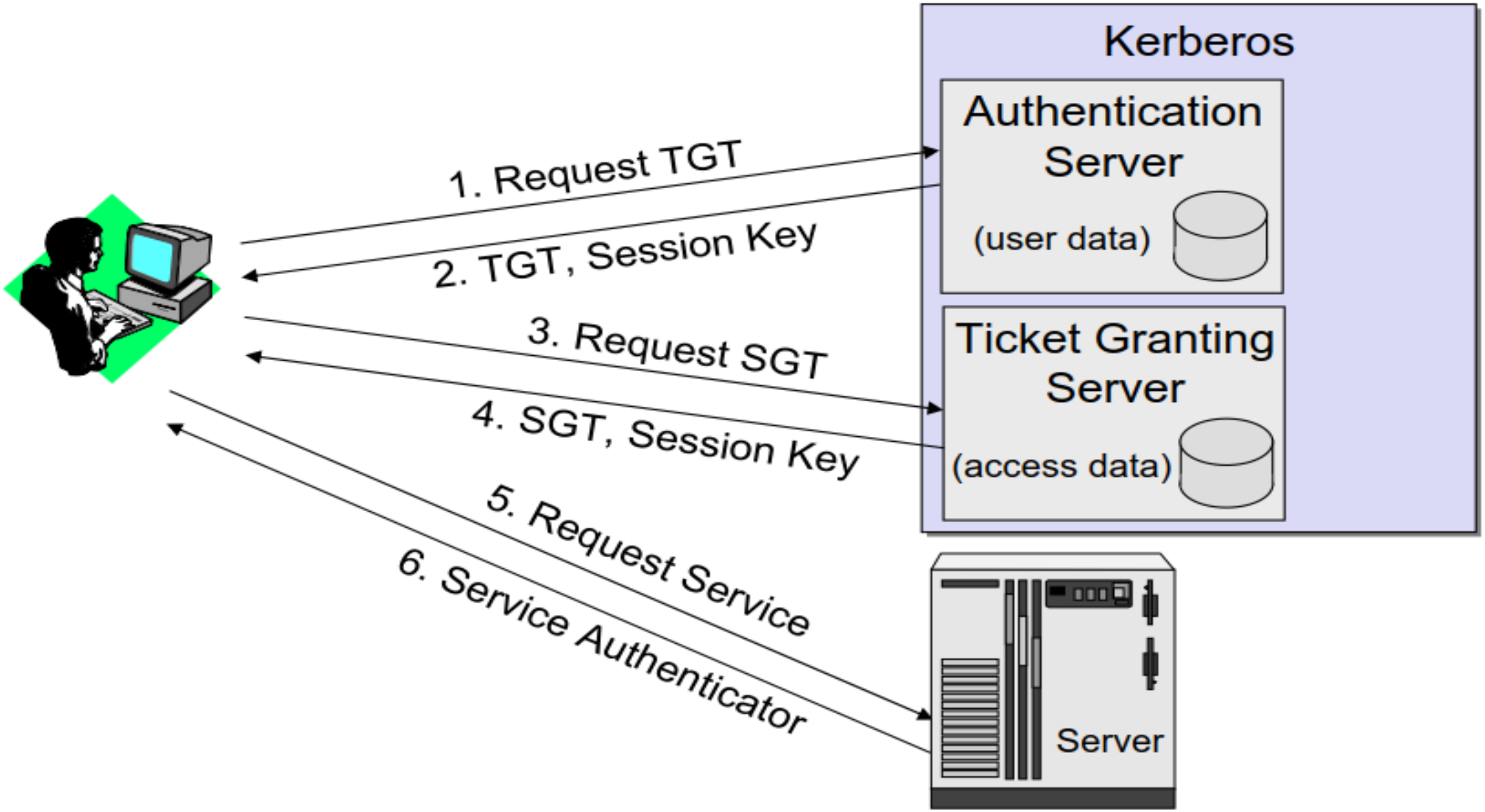
Bob

$(i_A, \{r_A, K_{A,B}\}_{K_{A,TTP}}, \{r_B, K_{A,B}\}_{K_{B,TTP}})$

$(i_A, \{r_A, K_{A,B}\}_{K_{A,TTP}})$

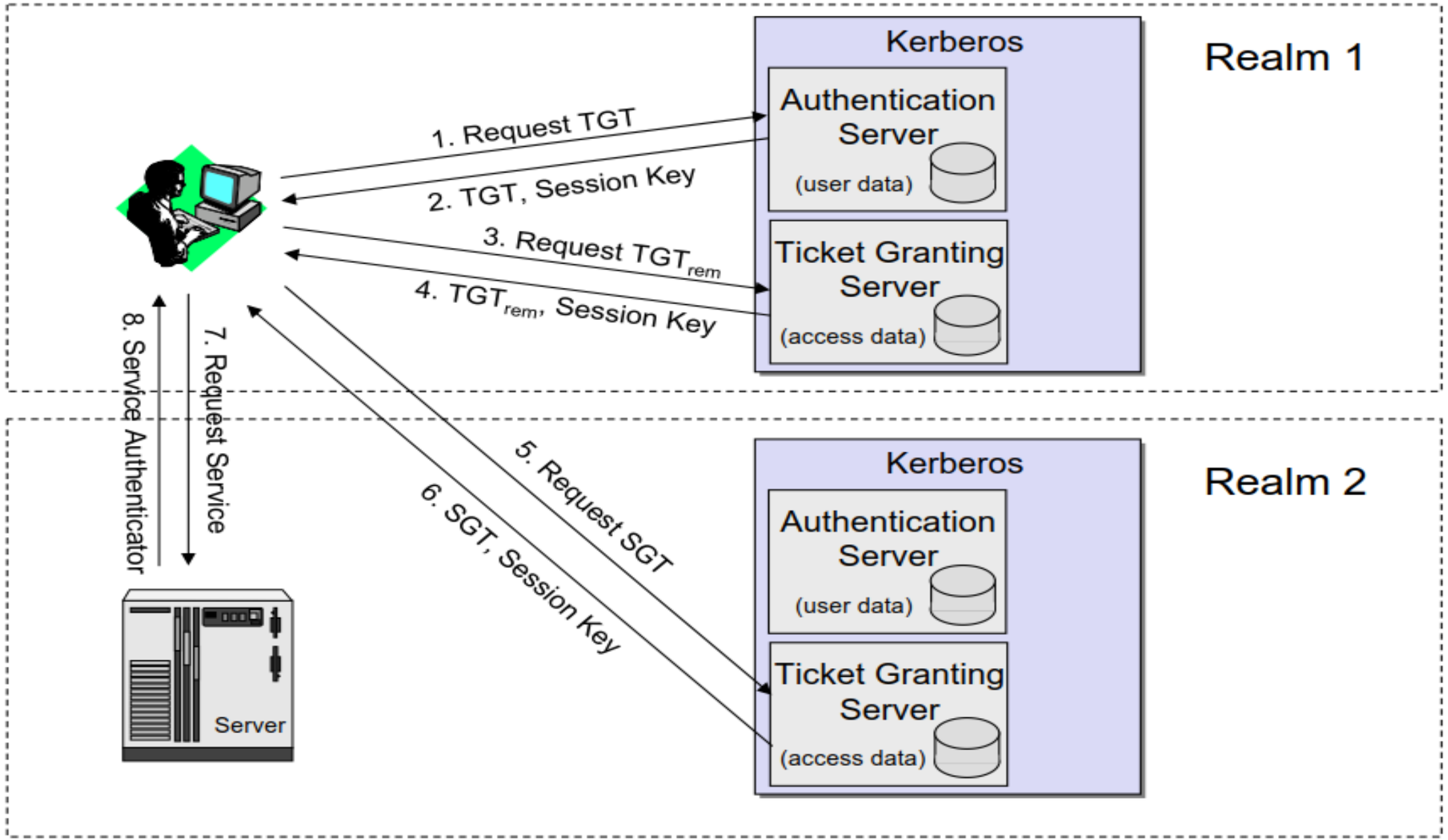
Kerberos


Authentication
Server (AS)
auth
request
A,B
Client/TGS
TGT
Client
C, D
TGT
authenticator
E, F
Client_to_server ticket
Client/server
Service
Server (SS)
E, G
Client_to_server ticket
authenticator
H
time auth



Accessing a Service with Kerberos Version 4 - Protocol Overview

Multiple Domain Kerberos (2)



Crypto++® Library 5.6.5

Crypto++ Library is a free C++ class library of cryptographic schemes. The library contains the following algorithms:

Algorithm	Name
authenticated encryption schemes	GCM, CCM, EAX, OCB
high speed stream ciphers	ChaCha (ChaCha8/12/20), Panama, Sosemanuk, Salsa20, XSalsa20
AES and AES candidates	AES (Rijndael), RC6, MARS, Twofish, Serpent, CAST-256
other block ciphers	ARIA, IDEA, Triple-DES (DES-EDE2 and DES-EDE3), Camellia, SEED, Kalyna, RC5, Blowfish, TEA, Threefish, Skipjack, SHACAL-2, XTEA
block cipher modes of operation	ECB, CBC, CBC ciphertext stealing (CTS), CFB, OFB, counter mode (CTR)
message authentication codes	VMAC, HMAC, GMAC (GCM), CMAC, CBC-MAC, DMAC, Two-Track-MAC, BLAKE2 (BLAKE2b, BLAKE2s), Poly1305, SipHash
hash functions	BLAKE2 (BLAKE2b, BLAKE2s), Keccack (F1600), SHA-1, SHA-2, SHA-3, Tiger, WHIRLPOOL, RIPEMD-128, RIPEMD-256, RIPEMD-160, RIPEMD-320
public-key cryptography	RSA, DSA, Determinsitic DSA, ElGamal, Nyberg-Rueppel (NR), Rabin-Williams (RW), EC-based German Digital Signature (ECGDSA), LUC, LUCELG, DLIES (variants of DHAES), ESIGN
padding schemes for public-key systems	PKCS#1 v2.0, OAEP, PSS, PSSR, IEEE P1363 EMSA2 and EMSA5
key agreement schemes	Diffie-Hellman (DH), Unified Diffie-Hellman (DH2), Menezes-Qu-Vanstone (MQV), Hashed MQV (HMQV), Fully Hashed MQV (FHMQV), LUCDIF, XTR-DH
elliptic curve cryptography	ECDSA, Determinsitic ECDSA, ECGDSA, ECNR, ECIES, ECDH, ECMQV
insecure or obsolescent algorithms retained for backwards compatibility and historical value	MD2, MD4, MD5, Panama Hash, DES, ARC4, SEAL 3.0, WAKE-OFB, DESX (DES-XEX3), RC2, SAFER, 3-WAY, GOST, SHARK, CAST-128, Square