Τεχνολογίες Blockchain & Αποκεντρωμένες Εφαρμογές

http://msnlab.uom.gr

Διάλεξη #02

Υπόβαθρο Blockchain

MSNlab

Ποιές περιοχές συνδυάζονται στο Blockchain

- Συνδυάζονται στοιχεία από:
  - Κρυπτογραφία
    - Για ασφάλεια στις συναλλαγές
  - Θεωρία Παιγνίων
    - Για λύσεις στο πρόβλημα των Βυζαντινών Στρατηγών
  - Επιστήμη Υπολογιστών
    - Για χρήσιμες δομές και μηχανισμούς

Περιεχόμενα

- Στοιχεία Κρυπτογραφίας
- Θεωρία Παιγνίων
- Επιστήμη Υπολογιστών
- Πώς συνδυάζονται τα προηγούμενα στο Blockchain

Εισαγωγή

- Η Κρυπτογραφία υπάρχει περισσότερο από 2.000 χρόνια ως περιοχή
- Στόχοι:
  - Εμπιστευτικότητα (Confidentiality)
  - Ακεραιότητα Δεδομένων (Data Integrity)
  - Αυθεντικοποίηση (Authentication)
  - Μη-άρνηση (Non-repudiation)

MSNlab

Βασική Ορολογία

- Plaintext: Το αρχικό (μη κρυπτογραφημένο, αναγνώσιμο) μήνυμα / κείμενο
- Ciphertext: Το κρυπτογραφημένο μήνυμα / κρυπτοκείμενο
- Key: Το κλειδί για κρυπτογράφηση ή/και για αποκρυπτογράφηση

Βασική Διαδικασία

- Εάν *m* το μήνυμα, *k* το κλειδί, **E** ο αλγόριθμος κρυπτογράφησης και **D** ο αλγόριθμος αποκρυπτογράφησης, έχουμε:
  - Ciphertext = $c = \mathbf{E}(k, m)$
  - Plaintext = $m = \mathbf{D}(k, c)$
- Οι αλγόριθμοι **E** και **D** μπορούν να ταυτίζονται
- Κεντρική ιδέα: Οποιοσδήποτε αντίπαλος πρέπει, εκτός από το κρυπτογραφημένο μήνυμα, να γνωρίζει και τον αλγόριθμο και το κλειδί, για να διαβάσει το αρχικό μήνυμα

Δύο Βασικές Κατηγορίες Κρυπτογραφίας

- Συμμετρική Κρυπτογραφία (Symmetric)

- Ασύμμετρη Κρυπτογραφία (Asymmetric)
  - Γνωστή και ως Δημοσίου Κλειδιού (Public Key)

Συμμετρική: βασικά βήματα

- Μεταξύ αποστολέα και παραλήπτη υπάρχει ένα κοινό (μυστικό) κλειδί *k*
  - Υποτίθεται ότι αυτό έχει σταλεί μέσω ασφαλούς καναλιού

- Βήματα Αποστολέα:
  - (1) $c = \mathbf{E}(k, m)$ (2) Αποστολή *c*
- Βήματα Παραλήπτη:
  - (1) Λήψη *c* (2) $m = \mathbf{D}(k, c)$

Αρχή του Kerckhoff

- Ένα Κρυπτοσύστημα* θα πρέπει να είναι ασφαλές ακόμα και εάν τα πάντα για αυτό – εκτός από το κλειδί – είναι δημοσίως γνωστά
  - Άρα ακόμα και εάν οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης είναι γνωστοί και υποκλαπεί κάποιο κρυπτογραφημένο μήνυμα, να μην είναι είναι δυνατή η μετατροπή του σε αναγνώσιμη μορφή χωρίς το κλειδί

---

* Σουίτα (σύνθεση) από αλγορίθμους κρυπτογράφησης που χρειάζονται για την παροχή ορισμένων υπηρεσιών ασφαλείας

Συμμετρική: σημαντικά στοιχεία

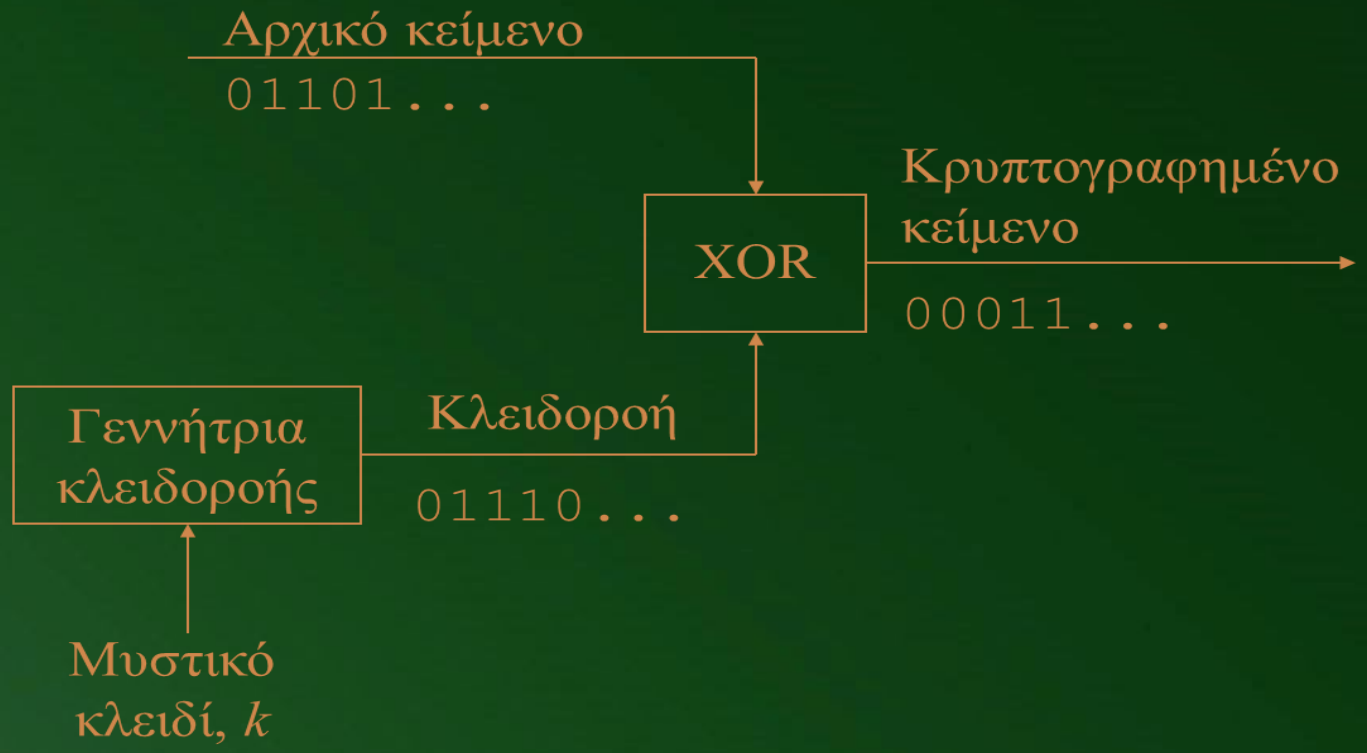
- Η Συμμετρική κρυπτογραφία χρησιμοποιείται ευρέως, επειδή:
  - είναι ταχύτερη (χρήσιμο για τεράστιο μέγεθος δεδομένων)
  - εξοικονομεί πόρους (HTTPS, υλοποιήσεις σε κινητά)

- Υπάρχουν δύο παραλλαγές κρυπταλγορίθμων (ciphers):
  - Ροής (stream)
  - Δέσμης (block)

Κρυπταλγόριθμοι Ροής έναντι Δέσμης

- Κρυπταλγόριθμοι Ροής (Stream Ciphers), π.χ. RC4
  - Μετατρέπουν κάθε σύμβολο του αρχικού κειμένου σε ένα σύμβολο κρυπτοκειμένου με ξεχωριστό κλειδί για κάθε σύμβολο (ακόμα και σε επίπεδο bit)
    - Απαιτείται ένα άπειρο πλήθος κλειδιών (π.χ., μίας χρήσης)
- Κρυπταλγόριθμοι Δέσμης (Block Ciphers), π.χ. DES
  - Το αρχικό κείμενο διαιρείται σε δέσμες (σχετικά μεγάλες ομάδες bit) σταθερού μεγέθους και χρησιμοποιείται το ίδιο κλειδί για κάθε δέσμη

Stream Cipher



- PNGR (Pseudo-Number GeneRator) με seed/κλειδί, που πρέπει να διανεμηθεί και στα δύο μέρη

Ιδιότητες των αλγορίθμων ροής

- Η κρυπτογράφηση γίνεται πολύ γρήγορα
- Δεν πολλαπλασιάζονται τα λάθη μετάδοσης
  - ένα λάθος στο κρυπτογραφημένο δίνει ένα λάθος στο αναγνώσιμο μήνυμα
- Δεν παρέχεται ανίχνευση μετατροπής του κρυπτομηνύματος.
  - ο υποκλοπέας αλλάζει ένα bit στο κρυπτογραφημένο κείμενο όντας σίγουρος ότι με αυτόν τον τρόπο θα αλλάξει μόνο το αντίστοιχο bit στο κείμενο που θα προκύψει από την αποκρυπτογράφηση του μηνύματος.

Ιδιότητες των αλγορίθμων ροής

- Το ίδιο κλειδί αν χρησιμοποιηθεί δυο φορές θα δώσει την ίδια κλειδοροή. Η συνήθης λύση είναι:
  - παράγεται ένα τυχαίο κλειδί (IV) πριν να κρυπτογραφηθεί το μήνυμα
    - με αυτό το κλειδί μετατρέπεται το (ήδη διανεμημένο) μυστικό κλειδί που εισάγεται στη γεννήτρια κλειδοροής.
  - κατόπιν, στέλνεται το κλειδί μηνύματος ως πρόθεμα (prefix) του κρυπτογραφημένου κειμένου.

Block Cipher

- Τα δεδομένα m χωρίζονται σε δέσμες των n bits:
  - $m_1, m_2, \ldots, m_q$
- Η τελευταία δέσμη m_q πιθανώς να μην περιέχει n bits, οπότε συμπληρώνεται με πρόσθετα bits (padding bits)

Προβλήματα Block Cipher

- Συνηθισμένα μεγέθη block: 64, 128, 256 bit
  - Με κλειδί *k* μήκους *r* bit, οι δυνατοί συνδυασμοί των bit του κλειδιού είναι μόλις 2^r
  - Βοηθά η επιλογή τυχαίων *r* bit για το κλειδί
- Η κρυπτογράφηση της ίδιας δέσμης με το ίδιο κλειδί παράγει πάντα το ίδιο αποτέλεσμα
  - Κίνδυνος διαρροής πληροφοριών για το κλειδί

Μειονεκτήματα των Block Cipher

- Πιο αργοί στην κρυπτογράφηση και αποκρυπτογράφηση έναντι των Stream Cipher
- Σφάλμα σε ένα bit μπορεί να αλλοιώσει μέρος ή ολόκληρη τη δέσμη κατά το μετασχηματισμό της

Αλλά και Πλεονεκτήματα…

- Μεγαλύτερη διάχυση
  - κάθε bit μιας δέσμης αρχικού κειμένου επηρεάζει διάφορα bit της αντίστοιχης δέσμης κρυπτοκειμένου
- Παραδείγματα Block Ciphers:
  - DES
  - 3DES
  - AES

DES (Data Encryption Standard)

- Τεχνική Block Cipher
- Κάθε block μεγέθους 64 bit
- Από/Κρυπτογράφηση με κλειδί 64 bit
  - Στην πράξη, 8 bit για parity check, 56 για κλειδί
- Ευάλωτο σε επίθεση brute-force
- Χρήσιμο όμως για κατανόηση άλλων τεχνικών

DES

- Η αποκρυπτογράφηση είναι ίδια με την αντίστροφη σειρά
- Μειονέκτημα το μικρό μήκος κλειδιού (56 bit)
- Ευάλωτος σε επιθέσεις εξαντλητικής αναζήτησης (brute force)
- Αναζητήθηκε λύση με τον 3DES

3DES

- Χρησιμοποιεί ζεύγη κλειδιών DES (k1, k2).
- Κρυπτογράφηση :
  - $c = e_{k1}(d_{k2}(e_{k1}(m)))$
- όπου d/e είναι μια απο/κρυπτογράφηση DES
- Αποκρυπτογράφηση με αντίστροφη διαδικασία
- Δεν είναι σημαντικά ασφαλέστερη από μια απλή κρυπτογράφηση DES

Συμμετρικοί Αλγόριθμοι προ AES

Αλγόριθμος	Μήκος Κλειδιού	Αριθμός Κύκλων	Μαθηματικές Πράξεις
DES	56 bits	16	XOR, σταθερά S-boxes
Triple DES	112 ή 168 bits	48	XOR, σταθερά S-boxes
IDEA	128 bits	8	XOR, πρόσθεση, πολλαπλασιασμός
Blowfish	Μεταβλητό μέχρι 448 bits	16	XOR, μεταβλητά S-boxes, πρόσθεση
RC5	Μεταβλητό μέχρι 2048 bits	Μεταβλητό μέχρι 255	Πρόσθεση, αφαίρεση, XOR, περιστροφή
CAST-128	40 μέχρι 128 bits	16	Πρόσθεση, αφαίρεση, XOR, περιστροφή, σταθερά S-boxes

MSNlab

NIST νέο πρότυπο

- 3DES: αργός σε υλοποιήσεις με χρήση λογισμικού και όχι σημαντικά ασφαλέστερος
- NIST (1999): αναζήτηση νέου πρότυπο κρυπτογράφησης με απαιτήσεις:
  - συμμετρικός αλγόριθμος δέσμης με κλειδί 128, 192, 256 bit
  - πιο ασφαλής από 3DES
  - δημόσια διαθέσιμος
  - να παραμένει ασφαλής για >30 χρόνια
- Κριτήρια αξιολόγησης:
  - ασφάλεια αλγορίθμων
  - κόστος υλοποίησης
  - απλότητα λειτουργίας

Αλγόριθμος Rijndael

- Από τους 15 που υποβλήθηκαν, από 10 διαφορετικές χώρες, επιλέχθηκε ο **Rijndael**:
  - Μεταβλητό μήκος block: 128, 192, 256 bits
  - Μεταβλητό μήκος κλειδιού: 128, 192, 256 bits
  - Μεταβλητός αριθμός επαναλήψεων: 10, 12, 14
    - Ο αριθμός των επαναλήψεων εξαρτάται από το μήκος κλειδιού/block

AES – Βασικά στοιχεία

- Advanced Encryption Standard (προτυποποίση του Rijndael)
- Symmetric Block Cipher, αλλά δεν βασίζεται σε δίκτυο Feistel
- Χρησιμοποιεί δίκτυο substitution-permutation
- Επιτυγχάνει μεγαλύτερη ταχύτητα και μεγαλύτερη ασφάλεια
- Μέγεθος block: 128 bit
- Μέγεθος κλειδιού: 128 (AES-128), 192 (AES-192), και 256 (AES-256) bit

AES - Λεπτομέρειες

- Η κάθε έκδοση έχει και διαφορετικό πλήθος γύρων:
  - AES-128, 10 γύροι
  - AES-192, 12 γύροι
  - AES-256, 14 γύροι
- Η αποκρυπτογράφηση δεν είναι παρόμοια με την κρυπτογράφηση
  - είναι αντίστροφη ως προς τους γύρους

Κρυπτογραφία Συμμετρικού Κλειδιού

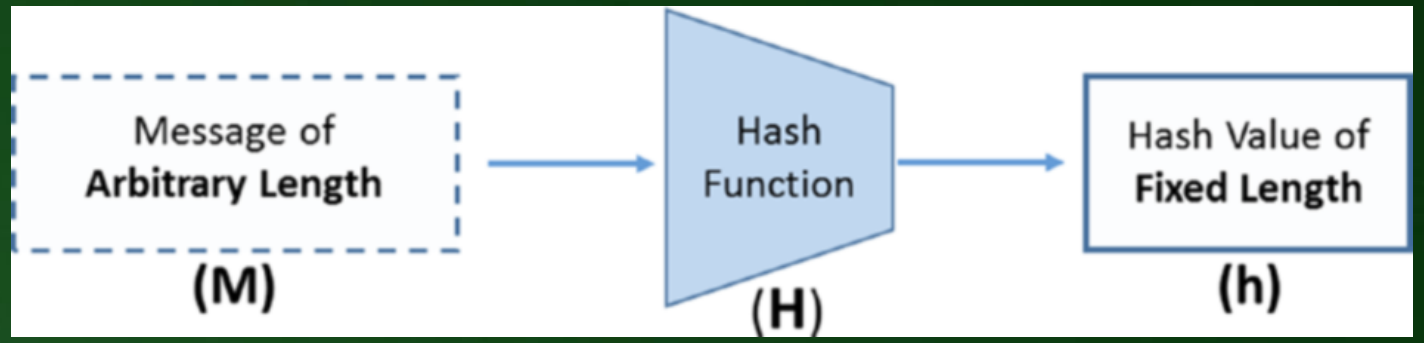
- Οι κυριότερες προκλήσεις είναι:
  - Διανομή κλειδιού μεταξύ αποστολέα/παραλήπτη
  - Αποστολέας/Παραλήπτης χρειάζεται να εμπιστεύονται ο ένας τον άλλον
    - Αν κάποιος τρίτος το έχει, το σύστημα αποτυγχάνει
  - Δίκτυο από n κόμβους χρειάζεται να διαχειρίζεται $n(n–1)/2$ ζεύγη κλειδιών
  - Είναι καλό να αλλάζουμε το κλειδί για κάθε σύνοδο
  - Συχνά χρειάζεται ένα τρίτο μέρος για αποδοτική διαχείριση κλειδιών

Συναρτήσεις Κατακερματισμού (ΣΚ)

- Cryptographic Hash Functions
  - Ειδική κατηγορία των ΣΚ (Hash Functions), κατάλληλες για κρυπτογραφικό πρωτόκολλο
  - Χρησιμοποιούνται σε
    - κρυπτογραφικά πρωτόκολλα
    - εφαρμογές ασφάλειας, όπως οι Ψηφιακές Υπογραφές
    - message authentication code (MAC)

Συναρτήσεις Κατακερματισμού (ΣΚ)

- Τρόπος λειτουργίας



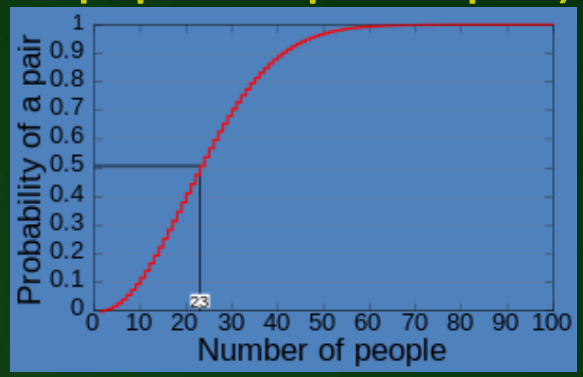
- Hash - Message Digest - Fingerprint

Βασικές Ιδιότητες ΣΚ

- Οιοδήποτε μέγεθος εισόδου, αλλά σταθερό μέγεθος εξόδου (συμπίεση)
- Αποδοτικός υπολογισμός εξόδου για οιοδήποτε μήνυμα
- Ίδια έξοδος για ίδια είσοδο
- Ανέφικτος ο υπολογισμός εισόδου από έξοδο (εκτός εάν δοκιμάσουμε όλα τα δυνατά μηνύματα)
- Οποιαδήποτε μικρή αλλαγή στην είσοδο πρέπει να επηρεάζει πολύ την έξοδο

Ιδιότητες Ασφάλειας ΣΚ -1

- Αντοχή σε Συγκρούσεις (Collision resistance)
  - Ανέφικτη η εύρεση 2 διαφορετικών τιμών εισόδου X και Y που να παράγουν ίδια τιμή hash: H (X) = H (Y)
  - Στην πράξη όχι αδύνατον, αλλά πολύ δύσκολο:
    - Αν η έξοδος έχει μήκος 256 bit: maximum 2^{256} τιμές hash
    - Με Επίθεση Γενεθλίων (Birthday Attack), δυνατή με κβαντικούς υπολογιστές, είναι πιθανό να βρεθεί μια σύγκρουση δοκιμάζοντας $2^{128} + 1$ εισόδους (birthday bound: $2^{n/2}$)



Ιδιότητες Ασφάλειας ΣΚ -2

- Αντοχή σε Προαπεικόνιση (Preimage resistance / “hiding”)
  - Εάν X η είσοδος και hash = H(X), τότε είναι υπολογιστικά αδύνατη η αντιστροφή: να βρούμε το X από το H(X)
    - Μονοκατευθυντική λειτουργία
    - Γενικά, πρέπει η είσοδος X να συνενώνεται με (ψευδο)τυχαία είσοδο “r” (nonce) μιας χρήσης για να είναι πρακτικά αδύνατο να βρούμε το X από το H (r || X)
      - Με r 256 bit, η πιθανότητα επιτυχούς προσπάθειας εύρεσης είναι $1 / 2^{256}$

Ιδιότητες Ασφάλειας ΣΚ -3

- Αντοχή σε 2η Προαπεικόνιση (2nd Preimage resistance)
  - Δοθείσας εισόδου X και της εξόδου H(X), είναι πρακτικά αδύνατο να βρούμε είσοδο Y, έτσι ώστε H(X) = H(Y)
- Puzzle Friendliness
  - Ιδιότητα που προκύπτει από τις προηγούμενες
  - Δεν υπάρχει σύντομη οδός για τη λύση και ο μόνος τρόπος είναι να διατρέξουμε όλες τις δυνατές επιλογές στο σύνολο των εισόδων

Διαδεδομένες Συναρτήσεις Κατακερματισμού -1

- Οικογένεια MD (Message Digest)
  - Δέσμη (block): 512 bit
  - Σύνοψη (digest): 128 bit
- Μέλη
  - MD4
    - RIPEMD
  - MD5
  - MD6

Διαδεδομένες Συναρτήσεις Κατακερματισμού -2

- Οικογένεια SHA (Secure Hash Algorithm)
- Μέλη
  - SHA-0, SHA-1
    - Δέσμη (block): 512 bit
    - Σύνοψη (digest): 160 bit
  - Από το 2010: SHA-2, SHA-3

SHA-2

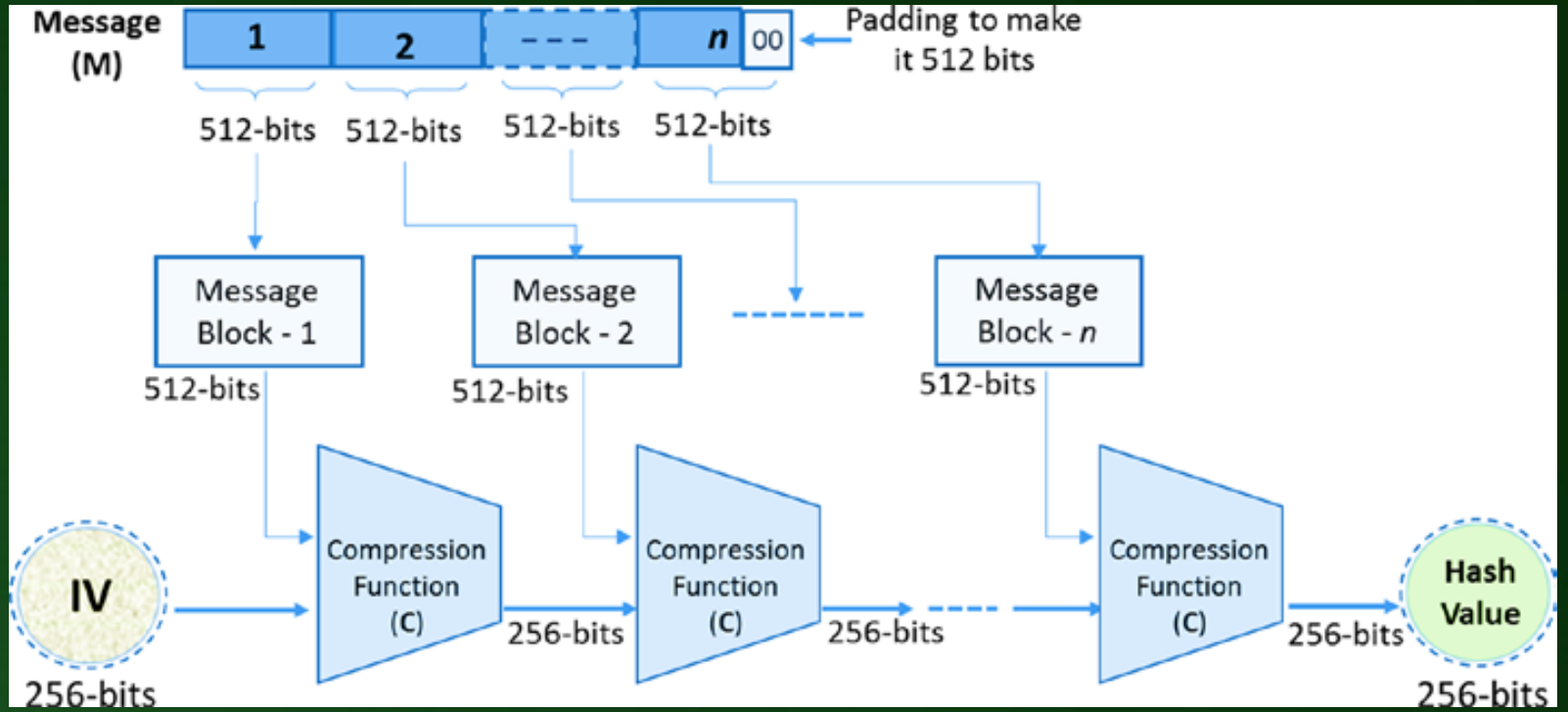
- Οικογένεια SHA-2:
- Βασικά μέλη:
  - SHA-256, SHA-512
- Παραλλαγές τους:
  - SHA-224 (SHA-256 truncated)
  - SHA-384, SHA-512/224, SHA-512/256 (SHA-512 truncated)

SHA-1 & SHA-2

Algorithm	Message Size (bits)	Block Size (bits)	Word Size (bits)	Message Digest Size (bits)
SHA-1	$< 2^{64}$	512	32	160
SHA-224	$< 2^{64}$	512	32	224
SHA-256	$< 2^{64}$	512	32	256
SHA-384	$< 2^{128}$	1024	64	384
SHA-512	$< 2^{128}$	1024	64	512
SHA-512/224	$< 2^{128}$	1024	64	224
SHA-512/256	$< 2^{128}$	1024	64	256

SHA-256 & SHA-512

- Σύνταξη (construction) Merkle-Damgard
- SHA-256
  - 512-bit blocks
  - 16 x 32-bit words
  - 64 rounds
- SHA-512
  - 1024-bit blocks
  - 16 x 64-bit words
  - 80 rounds



RIPEMD-160

- Οικογένεια: RIPEMD-128, RIPEMD-256, and RIPEMD-320
- RIPEMD-160: παραλλαγή του MD4
  - Merkle–Damgård construction
  - Είσοδος με δέσμες 512-bit και padding
  - Έξοδος 160-bit hash (αναπαράσταση με 40-ψήφιους δεκαεξαδικούς αριθμούς)
  - Λειτουργία συμπίεσης με 80 βήματα, σε 2 παράλληλες γραμμές με 5 γύρους των 16 βημάτων (5 × 16 = 80), πάνω σε 16 x 32-bit λέξεις (=512-bit)
- Χρησιμοποιείται στο Bitcoin
  - μαζί με SHA-256 για την παραγωγή διευθύνσεων
  - για συντόμευση της εξόδου (hash value του SHA-256 στα 160 bit)

SHA-3

- Προτυποποίηση του αλγορίθμου Keccak από το NIST (2015)
- Συνύπαρξη με SHA-2 και συμπλήρωσή του
- Sponge construction
- Οικογένεια:
  - SHA3-224, SHA3-256, SHA3-384, SHA3 -512
  - extendable-output functions (XOF): SHAKE128 & SHAKE256
- Ρύθμιση μεταξύ ασφάλειας και απόδοσης
  - μέσω της παραμέτρου capacity

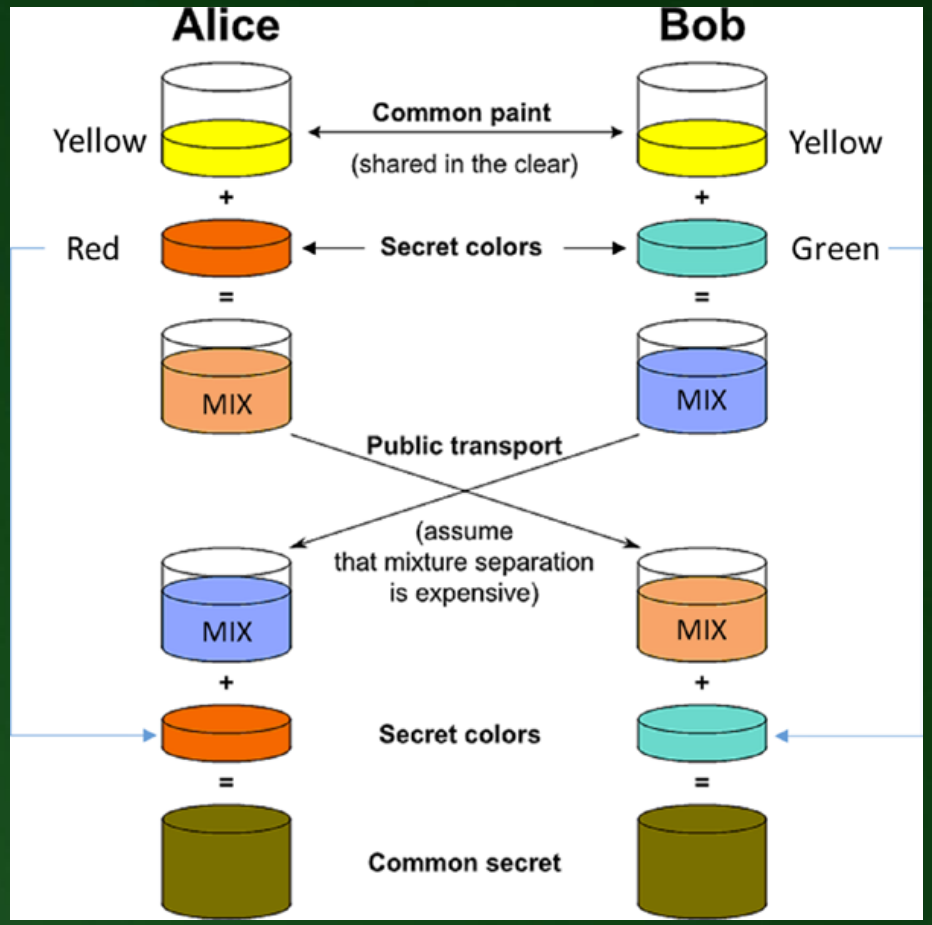
Εφαρμογές των Συναρτήσεων Hash

- Έλεγχος ακεραιότητας και αυθεντικότητας δεδομένων
- Δεικτοδότηση δεδομένων σε πίνακες συνόψεων για επιτάχυνση αναζήτησης
- Αυθεντικοποίηση χρηστών με συνθηματικά
- Υλοποίηση pseudorandom number generator
- Παραγωγή ψηφιακών υπογραφών και HMAC
- Αλγόριθμος proof of work (PoW) του Bitcoin
- Δημιουργία διευθύνσεων του Bitcoin

Ασύμμετρη Κρυπτογραφία / Δημοσίου Κλειδιού

- Όλα τα προηγούμενα σχήματα κρυπτογραφίας βασίσθηκαν σε συμμετρικά (μυστικά) κλειδιά.
- Το 1976, οι Diffie και Hellman ανακάλυψαν την ασύμμετρη κρυπτογραφία.
- Η ιδέα ήταν τα δύο μέρη να μην έχουν το ίδιο (μυστικό) αλλά διαφορετικά κλειδιά.
- Λύση στο πρόβλημα διαμοιρασμού κοινού κλειδιού.

Diffie-Hellman Key Exchange



Ασύμμετρη Κρυπτογραφία / Δημοσίου Κλειδιού

- Κάθε χρήστης παράγει το δικό του ζεύγος κλειδιών
  - Δημόσιο και Ιδιωτικό κλειδί
- Κατόπιν, γνωστοποιεί προς όλους το δημόσιο κλειδί του
- Οποιοσδήποτε κατέχει το δημόσιο κλειδί μπορεί να στείλει μυστικά μηνύματα, αλλά μόνο ο κάτοχος του ιδιωτικού κλειδιού μπορεί να τα αποκρυπτογραφήσει

Ασύμμετρη Κρυπτογραφία / Δημοσίου Κλειδιού

Είναι υπολογιστικά εύκολο:

- για κάποιο φορέα Β να δημιουργήσει ένα ζεύγος κλειδιών (δημόσιο κλειδί KU_b, ιδιωτικό κλειδί KR_b)
- για τον αποστολέα Α, γνωρίζοντας το δημόσιο κλειδί και το μήνυμα προς κρυπτογράφηση Μ, να δημιουργήσει το αντίστοιχο κρυπτογραφημένο μήνυμα $C = E_{KUb}(M)$
- για τον παραλήπτη Β να αποκρυπτογραφήσει το κρυπτογραφημένο μήνυμα C, χρησιμοποιώντας το ιδιωτικό του κλειδί, ώστε να ανακτήσει το αρχικό μήνυμα:

$$M = D_{KRb}(C) = D_{KRb}[E_{KUb}(M)]$$

Ασύμμετρη Κρυπτογραφία / Δημοσίου Κλειδιού

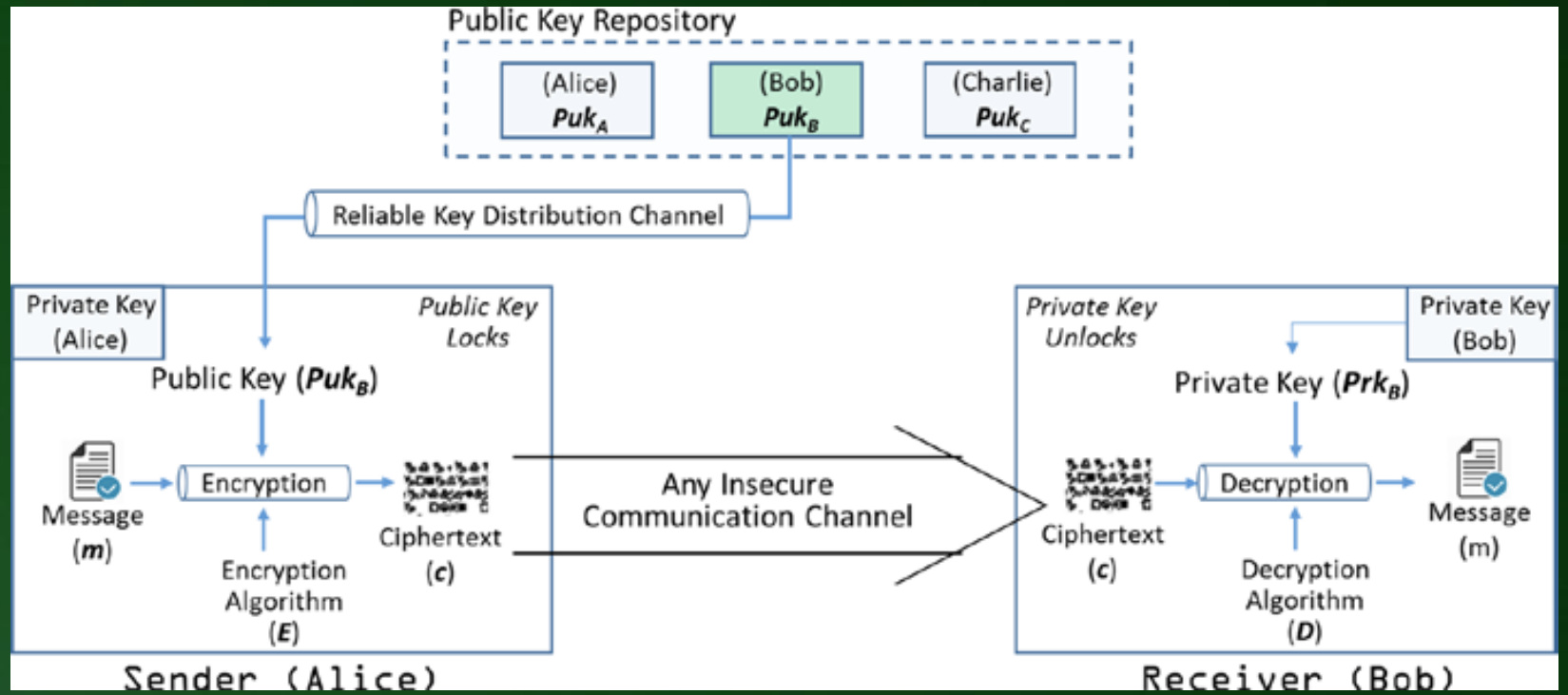
Είναι υπολογιστικά ανέφικτο για έναν επιτιθέμενο

- γνωρίζοντας το δημόσιο κλειδί KU_b να υπολογίσει το αντίστοιχο ιδιωτικό κλειδί KR_b.
- από το κρυπτογραφημένο κείμενο C να ανακτήσει το αρχικό κείμενο M.

Προαιρετικά: Οποιοδήποτε από τα δύο συσχετιζόμενα κλειδιά μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση, δηλαδή ισχύει:

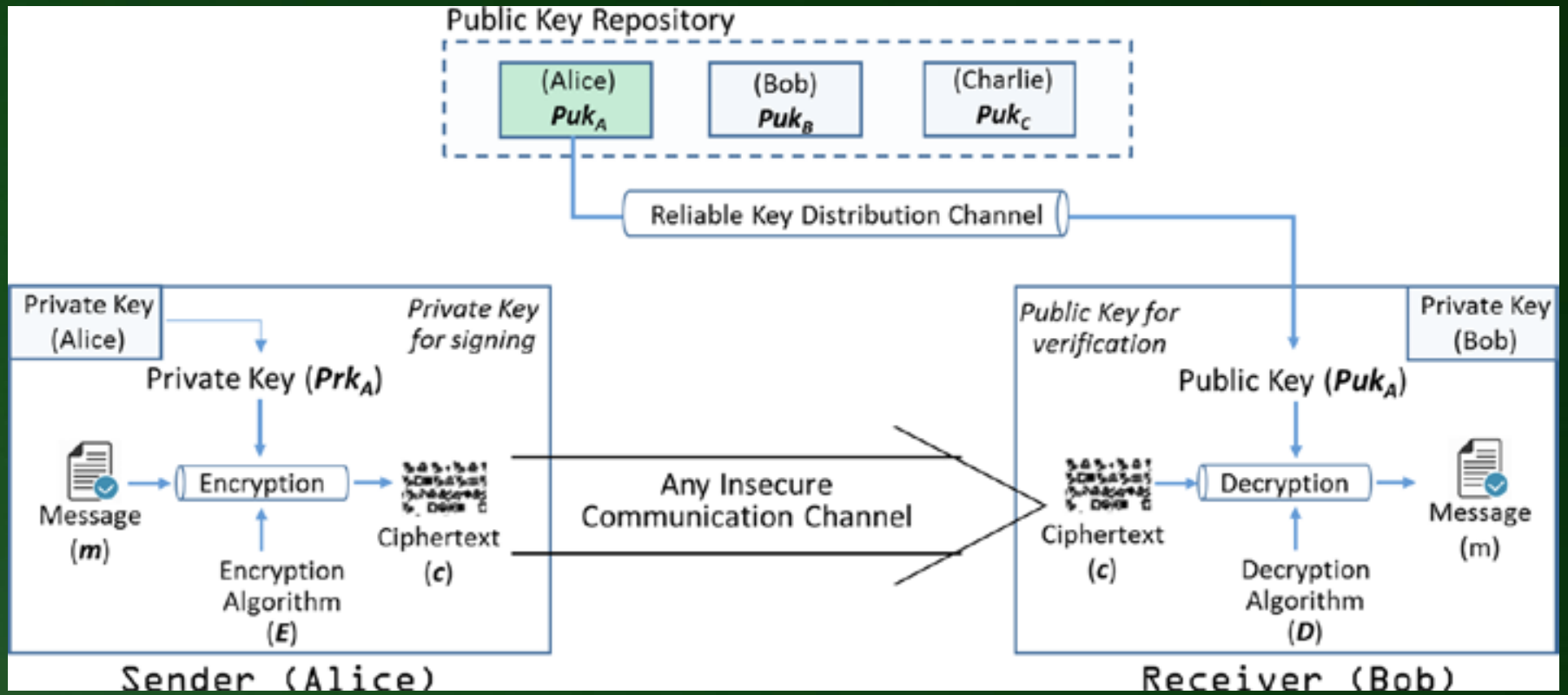
$$M = D_{KRb}[E_{KUb}(M)] = D_{KUb}[E_{KRb}(M)]$$

Ασύμμετρη Κρυπτογραφία / Δημοσίου Κλειδιού



Προστασία Εμπιστευτικότητας

Ασύμμετρη Κρυπτογραφία / Δημοσίου Κλειδιού



Προστασία Αυθεντικότητας

Ασύμμετρη Κρυπτογραφία / Δημοσίου Κλειδιού

- Τα Δημόσια Κλειδιά είναι γνωστά και προσβάσιμα από όλους
  - Κρυπτογράφηση μηνυμάτων
  - Επιβεβαίωση υπογραφών
- Τα Ιδιωτικά Κλειδιά είναι αποκλειστικά προσωπικά για τους κατόχους τους
  - Αποκρυπτογράφηση μηνυμάτων
  - Δημιουργία υπογραφών

Ασύμμετρη Κρυπτογραφία / Δημοσίου Κλειδιού

- Προβλήματα:
  - πώς μπορεί κανείς να είναι σίγουρος για την ταυτότητα του κατόχου ενός δημόσιου κλειδιού;
  - πώς διανέμονται στο κοινό τα δημόσια κλειδιά;
  - πώς ολοκληρώνεται ο κύκλος ζωής τους, όταν αυτό κριθεί αναγκαίο;

- Ανάγκη ύπαρξης μίας ‘Εμπιστης Τρίτης Οντότητας’ TTP, που διαχειρίζεται ‘Ψηφιακά Πιστοποιητικά’ DC

Πιστοποίηση (certification)

- Η διαδικασία της αντιστοίχισης και δέσμευσης ενός δημοσίου κλειδιού με ένα άτομο ή οργανισμό.
- Ψηφιακά πιστοποιητικά (digital certificates): τα μέσα ασφαλούς μετάδοσης των δημόσιων κλειδιών και των πληροφοριών κατόχου που σχετίζονται με αυτά.
- Η πιστοποίηση αποτελεί μια βασική λειτουργία των Υποδομών Δημοσίου Κλειδιού (ΥΔΚ) - PKI.

RSA

- Η πρώτη πρακτική εφαρμογή κρυπτογραφίας δημοσίου κλειδιού έγινε από τους Rivest, Shamir και Adleman (RSA) στα τέλη της δεκαετίας του 1970
- Η ιδέα βασίζεται στη δυσκολία εύρεσης των πρώτων παραγόντων (prime factors) πολύ μεγάλων ακεραίων
- Για κάποιο n, τα plaintext & ciphertext είναι ακέραιοι μεταξύ 0 και n – 1

RSA: Δημιουργία ζεύγους κλειδιών

- Επιλέγονται *p*, *q* : μεγάλοι πρώτοι αριθμοί (≥ 200 bits)
- Δημόσιο κλειδί: ζεύγος αριθμών *n* (modulus) και *e (*public exponent*)*, όπου:
  - $n = p \times q$
  - $e < (p-1)(q-1)$ και δεν διαιρεί ακριβώς το $(p-1)(q-1)$
    - δηλαδή ΜΚΔ$(e, (p-1)(q-1)) = 1$
- Ιδιωτικό κλειδί: ζεύγος αριθμών *n* και *d*, όπου:
  - $d = e^{-1} \pmod{(p-1)(q-1)}$
    - d και e είναι πολλαπλασιαστικοί αντίστροφοι modulo(p-1)(q-1),

RSA: Δημιουργία ζεύγους κλειδιών

- Το ζεύγος (*e*, *n*) γίνεται δημόσια γνωστό,

- ενώ τα *d*, *p* και *q* παραμένουν μυστικά (γνωστά μόνο στον κάτοχό τους)
  - αν και τα *p* και *q* μπορούν να διαγραφούν

RSA: Κρυπτογράφηση

- Για την κρυπτογράφηση ενός μηνύματος *m,* πρέπει αυτό να τεμαχισθεί σε δέσμες μήκους όχι μεγαλύτερου από αυτό του *n* (m ≤ n).

- Κάθε μια από αυτές τις δέσμες κρυπτογραφείται σε δέσμες c_i με το κλειδί κρυπτογράφησης (δημόσιο) και την ακόλουθη συνάρτηση:

$$c_i = \text{Encrypt}(m_i) = m_i^e \pmod{(n)}$$

RSA: Αποκρυπτογράφηση

- Για την αποκρυπτογράφηση χρησιμοποιείται το (ιδιωτικό) κλειδί αποκρυπτογράφησης και η ακόλουθη συνάρτηση:

$$m_i = \text{Decrypt}(c_i) = c_i^{\,d} \pmod{(n)}$$

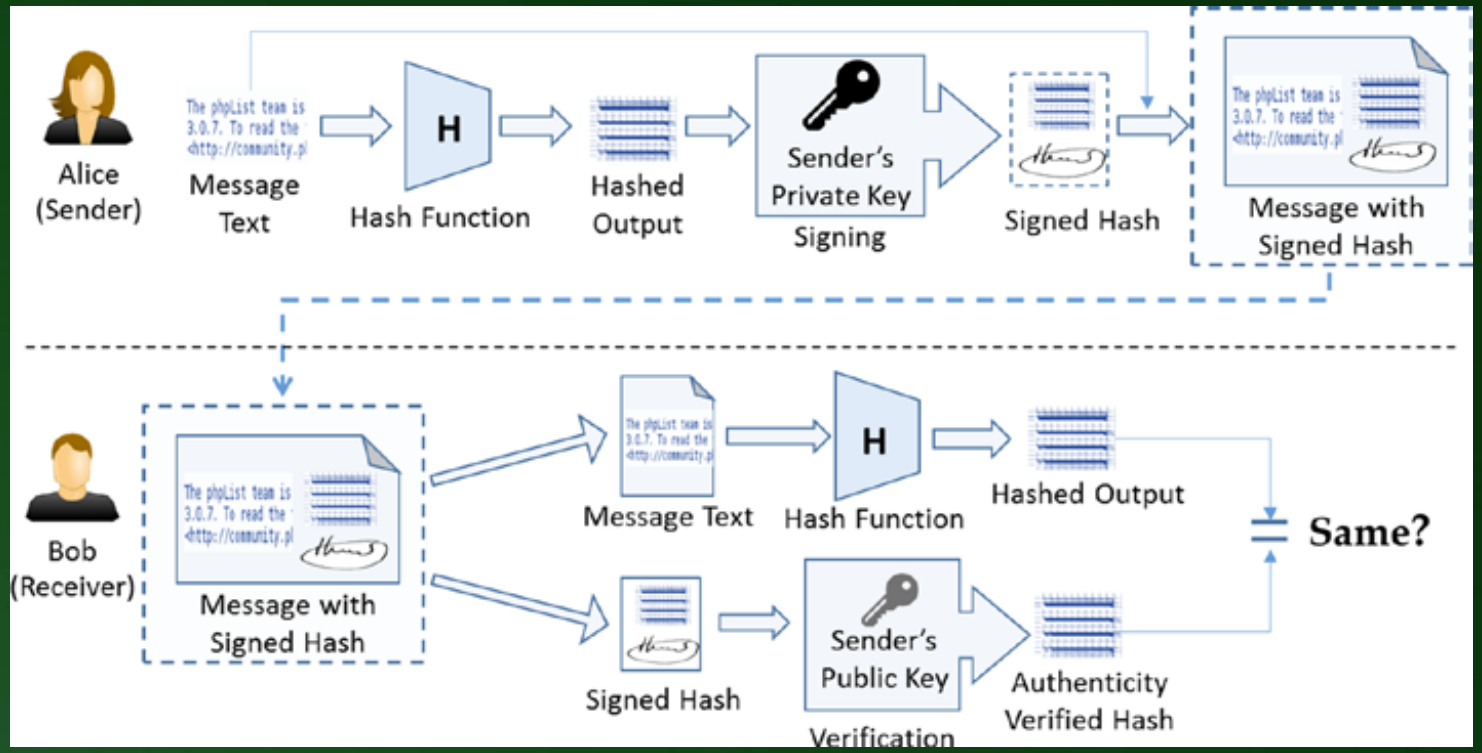
RSA: Ανθεκτικότητα

- Η ασφάλεια του RSA στηρίζεται στη δυσκολία εύρεσης του *d* με δεδομένα τα *n* και *e*
- Αν μπορέσουμε να παραγοντοποιήσουμε το ***n*** τότε μπορούμε να βρούμε τα *p* και *q*, οπότε να υπολογίσουμε το *d*
  - αν το πρόβλημα της παραγοντοποίησης μεγάλων αριθμών δεν ήταν άλυτο, ο RSA θα μπορούσε εύκολα να σπάσει.
- Κβαντικοί υπολογιστές?

DSA -Digital Signature Algorithm

- Σχεδιάστηκε από την NSA ως μέρος του προτύπου Digital Signature Standard (DSS)
- Αφορά την παραγωγή ψηφιακών υπογραφών μηνυμάτων
- Περιλαμβάνει φάσεις:
  - δημιουργίας κλειδιών
  - υπογραφής
  - επιβεβαίωσης
- Ιδιότητες ασφάλειας που παρέχει:
  - Αυθεντικότητα
  - Ακεραιότητα
  - Μη-απάρνηση

Digital Signature Algorithm



Κρυπτογραφία Ελλειπτικής Καμπύλης – ECC

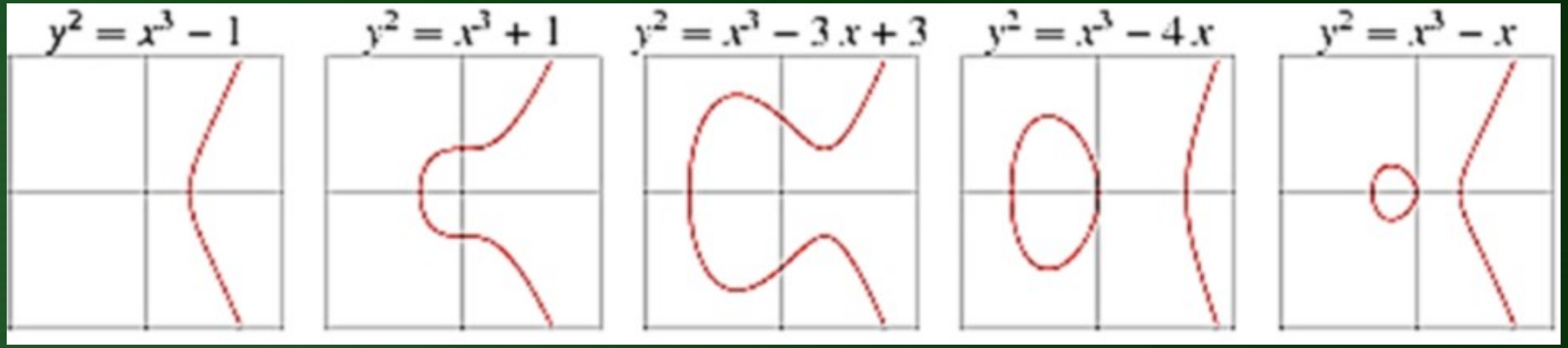
- Elliptic Curve Cryptography (ECC)
- Αποτελεί εξέλιξη της Κρυπτογραφίας Diffie-Hellman
- Θεωρείται ότι ένα κλειδί ECC 160-bit είναι το ίδιο ασφαλές όπως ένα κλειδί RSA 1024-bit
- Χρησιμοποιείται ευρέως σε συστήματα IoT, embedded, κλπ.

Ελλειπτικές Καμπύλες – Βασικά

- Μια ελλειπτική καμπύλη ικανοποιεί την εξίσωση:

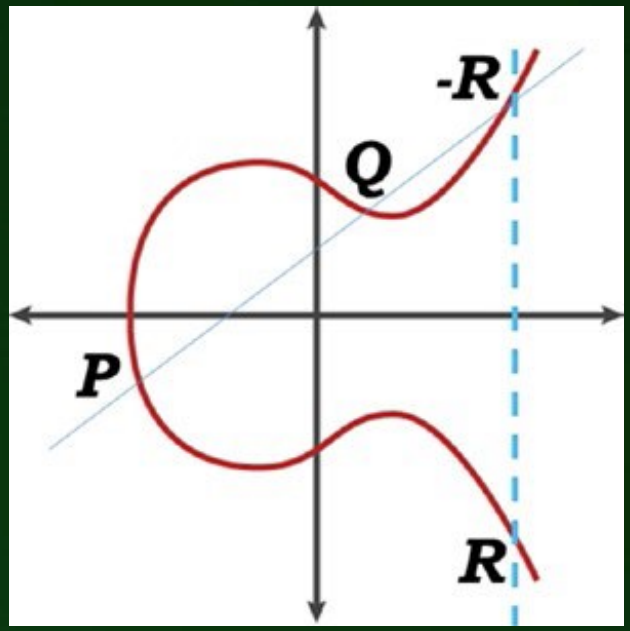
  $y^2 = x^3 + ax + b$ όπου $4a^3 + 27b^2 \neq 0$

  Παραδείγματα για διάφορες τιμές των a και b



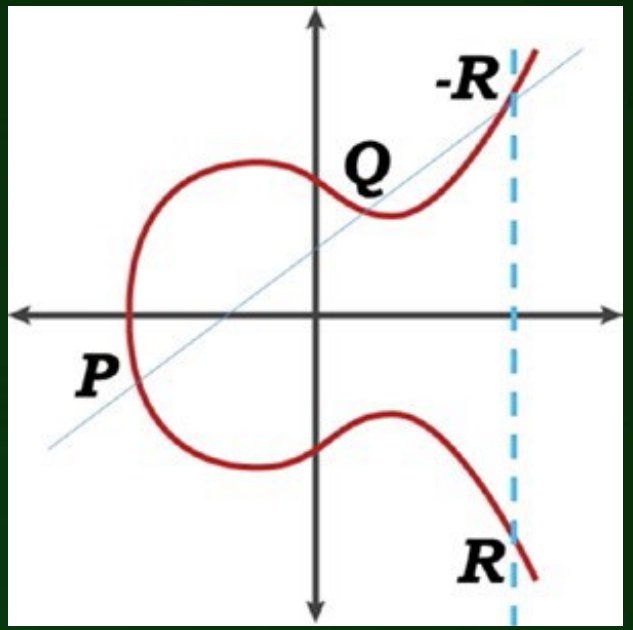
Ιδιότητες – (1)

- Είναι οριζόντια συμμετρικές
  - κατοπτρικές ως προς άξονα X
- Οιαδήποτε μη κατακόρυφη γραμμή μπορεί να τέμνει την καμπύλη σε *το πολύ 3 σημεία*



Ιδιότητες – (2)

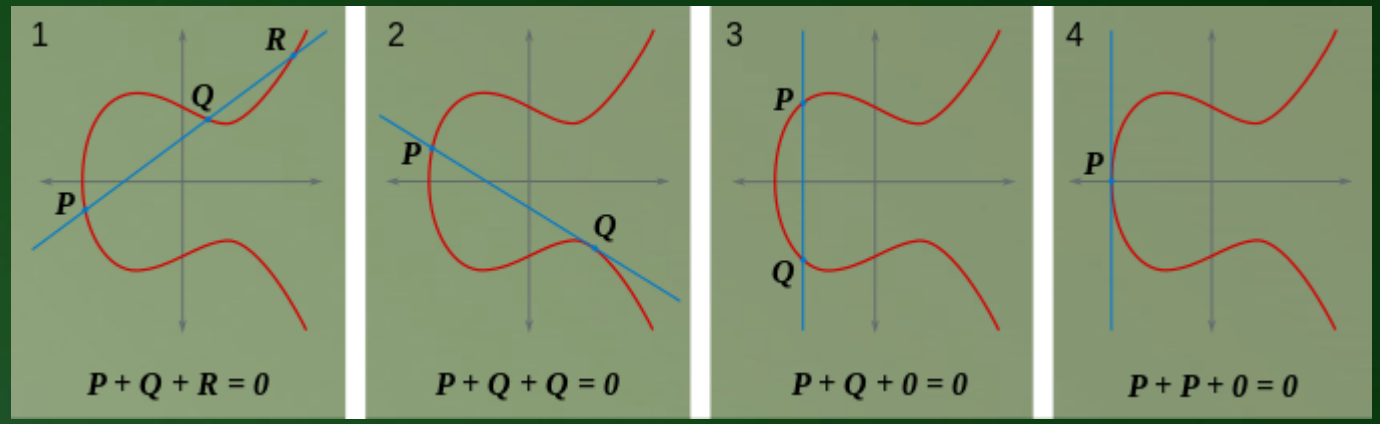
- Τα σημεία μιας ελλειπτικής καμπύλης αποτελούν μια *αβελιανή ομάδα*:
  - με πράξη την πρόσθεση **+**
  - με ουδέτερο στοιχείο το σημείο στο άπειρο **O**
    - βρίσκεται σε κάθε κατακόρυφη (≤ 2 σημεία τομής)
  - με ιδιότητες:
    - κλειστότητα,
    - προσεταιριστικότητα,
    - ύπαρξη αντιστρόφου στοιχείου,
    - ύπαρξη ουδέτερου στοιχείου,
    - αντιμεταθετικότητα



Πρόσθεση σημείων

3. Έστω δύο σημεία P και Q στην ελλειπτική καμπύλη
   - Εάν τραβήξουμε μέσω αυτών μία ευθεία γραμμή, αυτή τέμνει την καμπύλη σε ένα το πολύ ακόμα σημείο (έστω το R)
   - Η κατακόρυφη γραμμή από το R τέμνει την καμπύλη στο -R (κατοπτρικό του R) και:

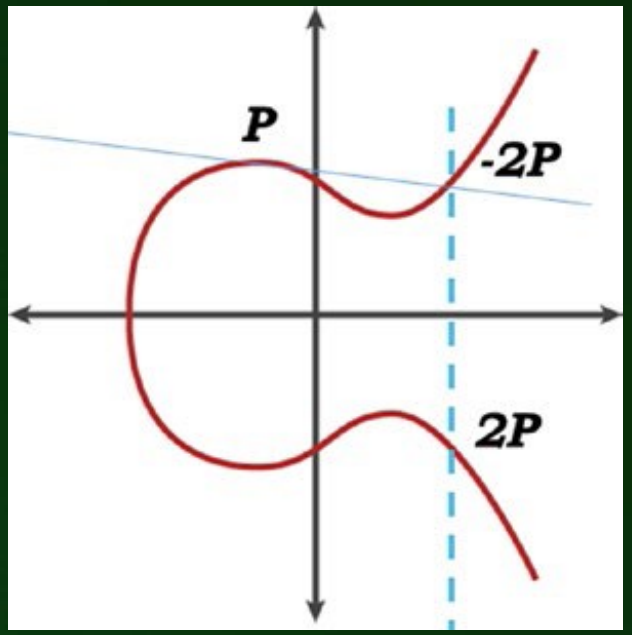
P + Q = -R ("Point Addition")



Διπλασιασμός σημείου

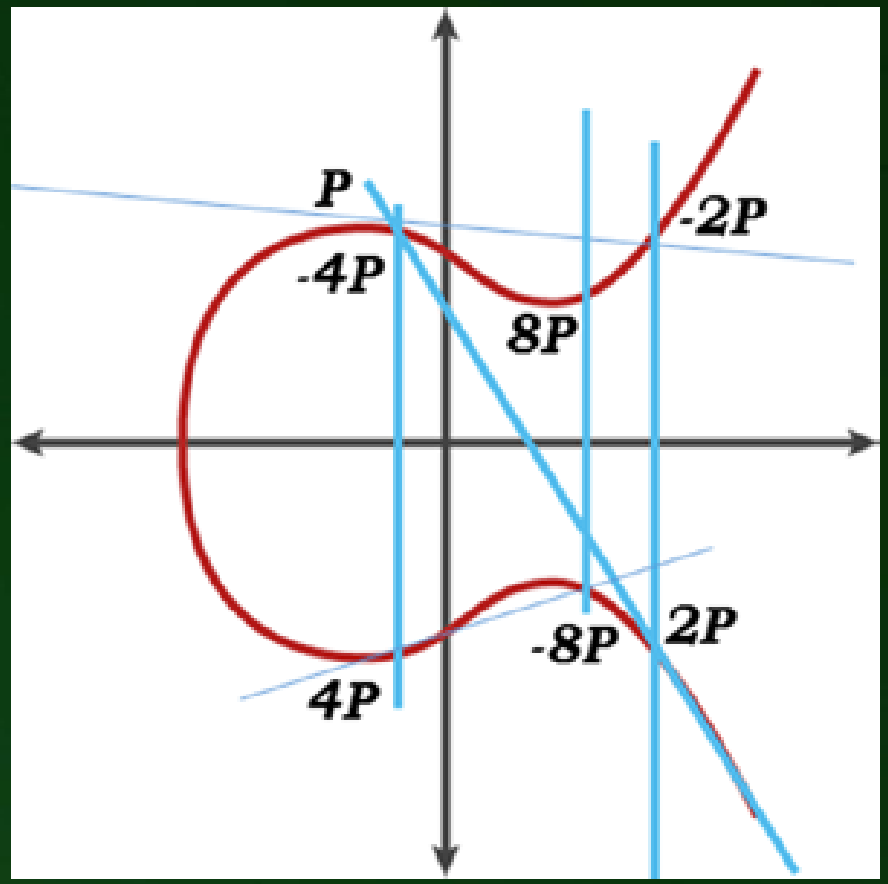
- Εάν την προηγούμενη διαδικασία δύο σημείων (P και Q) την εφαρμόσουμε για το ίδιο σημείο P (με την εφαπτομένη γραμμή), τότε έχουμε το “Point Doubling”

- Εδώ το -2P και με την κατακόρυφη το 2P



Πολλαπλασιασμός σημείου

- Εφαρμόζοντας το “Point Doubling” n φορές, καταλήγουμε σε διαφορετικά σημεία, όπως στο σχεδιάγραμμα



Χρησιμοποιούμενα Χαρακτηριστικά για ECC

- Εάν δοθούν το αρχικό και το τελικό σημείο, μετά από διαδοχικά “Point Doubling” και “Point Addition”, δεν υπάρχει τρόπος να βρει κανείς πόσες φορές εφαρμόσθηκαν, για να φθάσουμε στο τελικό σημείο, εκτός εάν δοκιμάσει για όλους τους πιθανούς συνδυασμούς, ένα προς ένα
  - Γνωστό και ως Πρόβλημα Διακριτών Λογαρίθμων για ECC (Discrete Logarithm Problem for ECC)

Elliptic Curve Digital Signature Algorithm (ECDSA)

- ECC χρησιμοποιείται για δημιουργία κλειδιών, αλλά συνδυάζεται με άλλες τεχνικές:
  - Elliptic Curve Diffie- Hellman (ECDH)
    - για ανταλλαγή κλειδιών
  - ECDSA
    - για ψηφιακή υπογραφή (π.χ., στο Bitcoin)

Elliptic Curve Digital Signature Algorithm (ECDSA)

- Τρία βασικά βήματα:
  - δημιουργία κλειδιών
  - δημιουργία υπογραφής
  - επιβεβαίωση υπογραφής

Symmetric vs. Asymmetric Key Cryptography

- Πρόβλημα η ανταλλαγή κλειδιών για τη συμμετρική κρυπτογράφηση – λύση η ασύμμετρη κρυπτογράφηση
- Αργή η ασύμμετρη κρυπτογράφηση – αποκρυπτογράφηση
- Στην ασύμμετρη κρυπτογράφηση τα κείμενα έχουν τη μορφή ακεραίων
- Η συμμετρική κρυπτογράφηση δεν παρέχει ψηφιακές υπογραφές
- Στην ασύμμετρη κρυπτογράφηση, κάθε μέρος πρέπει να έχει τουλάχιστον ένα ζεύγος κλειδιών, ανεξαρτήτως πλήθους κόμβων επικοινωνίας.
  - Πόσα κλειδιά χρειάζονται για ανά 2 επικοινωνία με n κόμβους;

Symmetric vs. Asymmetric Key Cryptography

Number of Participants	Number of Symmetric Keys	Number of Asymmetric Keys
2	1	4
4	6	8
10	45	20
50	1225	100
100	4950	200
1000	499500	2000