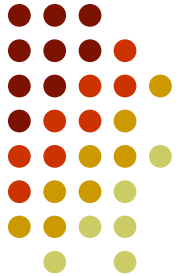
Εισαγωγή στο μάθημα της κρυπτογραφίας

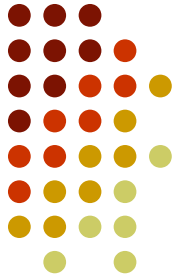
Λίγα λόγια για το μάθημα



Στόχοι του μαθήματος.

1. Να κατανοήσω βασικά κρυπτοσυστήματα, συμμετρικά και δημοσιού κλειδιού που έχουν εφαρμογή στα σύγχρονα κρυπτογραφικά πρωτόκολλα στο διαδίκτυο.
2. Να μάθω το απαραίτητο μαθηματικό υπόβαθρο που απαιτείται για την κατονόηση του RSA και Diffie-Hellman.
3. Να μάθω βασικά πράγματα για το πρωτόκολλο SSL/TLS.
4. Να μαθώ να υλοποιώ απλές επιθέσεις με χρήση Python/C/C++ στο RSA
5. Να μάθω βασικές αρχές για Pen Test! (extra bonus)

Λίγα λόγια για το μάθημα



Εργασία (Project) (50%)

Παρουσίαση ενός θέματος κρυπτογραφίας (bonus) (10%)

Στο τέλος γραπτές εξετάσεις (με σημειώσεις) (40%)

Θα υπάρξουν κάποια bonus με την μορφή εβδομαδιαίων εργασιών.

Προαπαιτούμενα

Εγκαταστήστε την Python (διανομή anaconda+jupyter)

Εγκαταστήστε μια διανομή του Linux!

Βιβλιογραφία

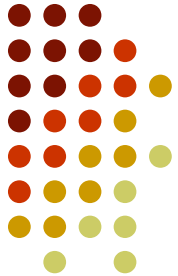
Βιβλία

1. *Υπολογιστική Κρυπτογραφία* (Κάλιππος)
2. Δίκτυα και ασφάλεια, Stalling (Εύδοξος)
3. Για τον ελεύθερο χρόνο σας

Κώδικες και μυστικά, S.Singh (καλό εισαγωγικό βιβλίο και αρκετά διασκεδαστικό)

4. Δείτε και στο Elearning

Που χρειάζεται η κρυπτογραφία;



Η κρυπτογραφία χρησιμοποιείται για να προστατεύει πληροφορίες σ'ένα υπολογιστικό σύστημα. Για παράδειγμα στις on-line συναλλαγές μας με μια τράπεζα και στην προστασία των κωδικών μας, τρέχουν πολλοί κρυπτογραφικοί αλγόριθμοι. Για την προστασία στρατιωτικών μυστικών, ιατρικών δεδομένων, βιομηχανικών μυστικών κ.λπ.

Η κρυπτογραφία όσο χρήσιμη είναι, τόσο δύσκολο είναι να υλοποιηθεί σωστά (η sony αποτελεί μια τέτοια περίπτωση που χρησιμοποίησε με λανθασμένο τρόπο κρυπτογραφικό σύστημα για να προστατέψει από την πειρατεία λογισμικό για την κονσόλα PS3). Σε αυτό το μάθημα θα δώσουμε έμφαση σε σύγχρονες εφαρμογές της κρυπτογραφίας.

Η κρυπτογραφία δεν είναι :

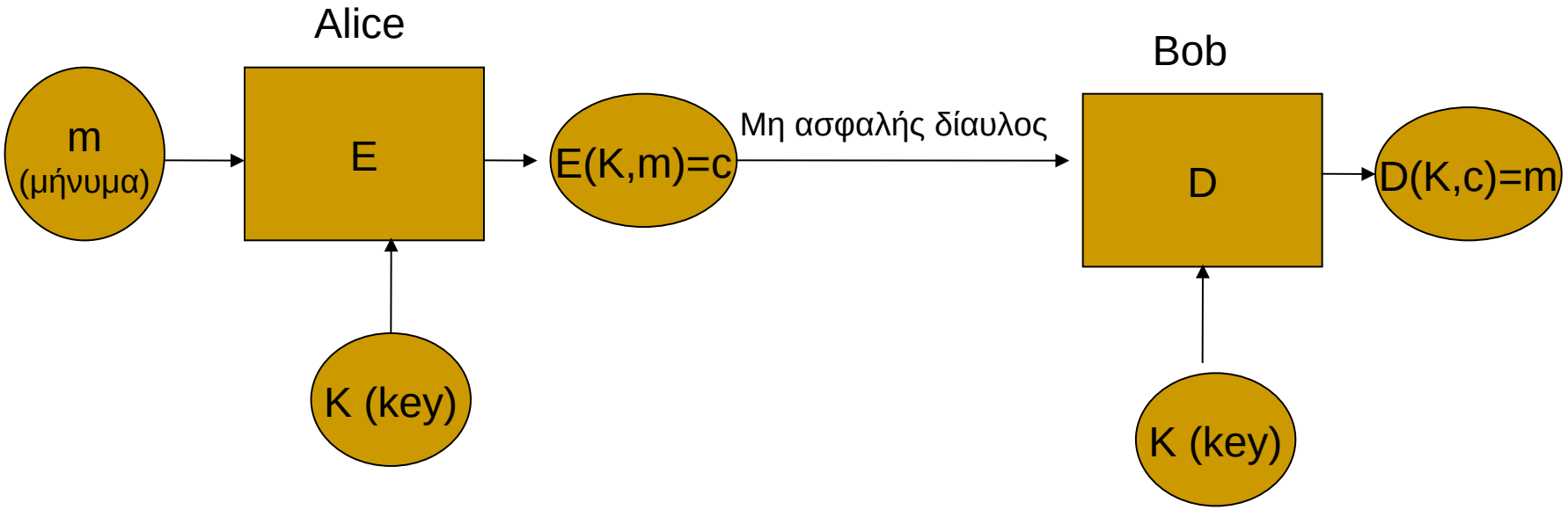
1. η λύση για όλα τα θέματα ασφαλείας
2. χρήσιμη αν δεν υλοποιηθεί σωστά

Η κρυπτογραφία χρησιμοποιείται πολύ συχνά

Web traffic : https (SSL/TLS)
Ασύρματα δίκτυα : 802.11i WPA 2
Προστασία δεδομένων : (DVD) CSS
Ηλεκτρονική Ψηφοφορία : Helios
Ανωνυμία στο διαδίκτυο : Tor, Tails (onion protocol)
Αποκεντρωμένες συναλλαγές : Bitcoin
Ψηφιακή υπογραφή : DSA,RSA,ECDSA
Κρυπτογράφηση e-mail : GPG

Συμμετρική Κρυπτογραφία

Την χρησιμοποιούμε για να κρυπτογραφήσουμε ένα μήνυμα.



SOS : Ο αλγόριθμος κρυπτογράφησης E και αποκρυπτογράφησης D είναι δημόσια γνωστοί.

Αρχή του Kerckhoff : Η ασφάλεια ενός κρυπτοσυστήματος δεν πρέπει να βασίζεται στη γνώση του κρυπτοσυστήματος, αλλά στη γνώση του μυστικού κλειδιού

Συμμετρική Κρυπτογραφία

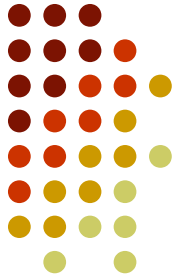
Ονομάζεται συμμετρική κρυπτογραφία διότι, τόσο η Alice όσο και ο Bob χρησιμοποιούν το **ίδιο** κλειδί κρυπτογράφησης και αποκρυπτογράφησης. Υπάρχουν συστήματα στα οποία αυτά τα δύο κλειδιά είναι διαφορετικά (π.χ. στο RSA). Γι'αυτό και ονομάζονται ασύμμετρα συστήματα κρυπτογράφησης.

Μερικοι αξιόπιστοι συμμετρικοί αλγόριθμοι είναι:

AES (Rijndael),CHACHA20,Twofish, Serpent,Blowfish,CAST5,IDEA

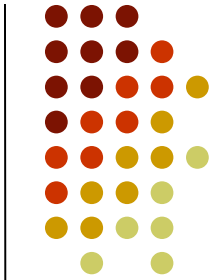
Εμείς θα δούμε ένα από τα πρώτα συμμετρικά συστήματα που υιοθέτησε η NSA ,που είναι το **DES** (Data Encryption Standard). Επίσης θα δούμε και το σύγχρονο σύστημα **AES.**

Ανακεφαλαίωση.
Τι είναι η κρυπτογραφία;



Ο “πυρήνας” ενός συστήματος κρυπτογραφίας αποτελείται από δύο μέρη

1. Παραγωγή κοινού μυστικού κλειδιού
2. Ασφαλή μετάδοση μηνύματος



Με την κατάλληλη χρήση των κρυπτογραφικών αλγορίθμων μπορώ:

1. να φτιάξω *ψηφιακές υπογραφές*.
2. https
3. να κάνω *ανώνυμη περιήγηση* (mix net, Tor).
4. *ssh* (secure shell)
5. να έχω *ανώνυμο ψηφιακό χρήμα* (bitcoin).
6. να *ψηφίζω ηλεκτρονικά*.
7. να κάνω *αποδείξεις μηδενικής γνώσης* (zero-knowledge proofs)
8. Post quantum κρυπτογραφικά συστήματα
9. Ομομορφική κρυπτογράφηση
10. Lightweight Cryptography

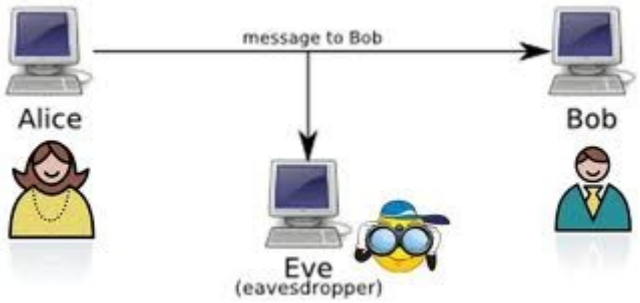
Ψηφιακή υπογραφή

Πολλές φορές χρειάζεται να υπογράψουμε ηλεκτρονικά ένα έγγραφο. Για παράδειγμα η αναφορά που συντάσσει ένας αστυνόμος πρέπει να υπογραφεί με τέτοιο τρόπο ώστε να βεβαιώνεται η ταυτότητα του. Σήμερα και στην Ελλάδα οι ψηφιακές υπογραφές έχουν νομική ισχύ, μέσα από μια σειρά νόμων.

Η ΑΠΕΔ είναι η αρχή πιστοποίησης του ελληνικού δημοσίου. Οι υπηρεσίες οι οποίες προσφέρονται από την εν λόγω υποδομή, δίνουν τη δυνατότητα στα στελέχη του Δημοσίου και τους πολίτες, με τη χρήση Ασφαλών Διατάξεων Δημιουργίας Υπογραφής (ΑΔΔΥ - etoken), να υπογράφουν ψηφιακά τις μεταξύ τους ηλεκτρονικές επικοινωνίες και συναλλαγές. Η ψηφιακή αυτή υπογραφή, σύμφωνα με το Π.Δ. 150/2001 (ΦΕΚ 125/Α΄/2001), επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο.

Μερικές μόνο αρχές πιστοποίησης μπορούν να εκδίδουν εγκεκριμένες (qualified) ψηφ. Υπογραφές. Οι εγκεκριμένες ψηφ. Υπογραφές έχουν την ισχύ της ιδιόχειρης υπογραφής. Φυσικά η ΑΠΕΔ, αλλά και το Α.Π.Θ. (διά της HARICA : υποδομή δημοσίου κλειδιού των ακαδημαικων ιδρυμάτων) καθώς και η εταιρεία Adacom. Π.χ. η ΑΠΕΔ εκδίδει δωρεάν ψηφιακές υπογραφές με κατάλληλη αίτηση (σε όλους τους έλληνες πολίτες) στην ψηφιακή πύλη ERMIS. Επίσης το ΑΠΘ εκδίδει δωρεαν ψηφ. υπογραφές στους υπαλλήλους του καθώς και στους φοιτητές.

Ασφαλής επικοινωνία SSL/TLS



Για παράδειγμα η Alice προσπαθεί να επικοινωνήσει με ασφάλεια με τον Bob. Αν η Έυα παρακολουθεί τη συνομιλία τους, το κρυπτογραφικό πρωτόκολλο *https* εγγυάται ότι δεν μπορεί η συνομιλία της Alice και του Bob να κλαπεί (*εμπιστευτικότητα).*

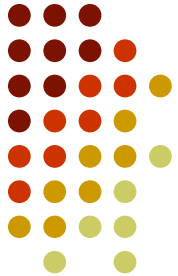
και επίσης δεν μπορεί η Έυα να παρέμβει και να αλλάξει την συνομιλία μας (*ακεραιότητα*). Οι Κρυπταναλυτές έχουν τον ρόλο της Έυας.

Το πρωτόκολλο SSL/TLS υλοποιείται σε δύο βήματα.

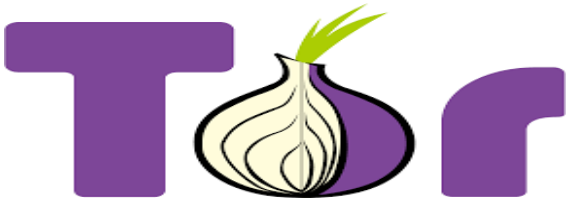
1. **Χειραψία (handshake).** Η χειραψία είναι ένα πρωτόκολλο που στο τέλος θα έχει δώσει ένα κοινό κλειδί στον Bob και την Alice. Η Έυα παρότι θα παρακολουθεί το κανάλι δεν θα μπορεί να υπολογιστικά γρήγορα να βρει το κλειδί. Το κοινό κλειδί παράγεται με χρήση της Κρυπτογραφίας Δημόσιου Κλειδιού (Public Key Cryptography).

2. **Record Layer.** Σε αυτό το βήμα η Alice και ο Bob ανταλλάσσουν μηνύματα κάνοντας χρήση του κοινού μυστικού κλειδιού. Στο βήμα αυτό διασφαλίζεται η *εμπιστευτικότητα και η ακεραιότητα.* Για να υλοποιηθεί αυτό το βήμα χρησιμοποιώ συμμετρική κρυπτογραφία για την *εμπιστευτικότητα* και συμμετρική κρυπτογραφία για την *ακεραιότητα*.

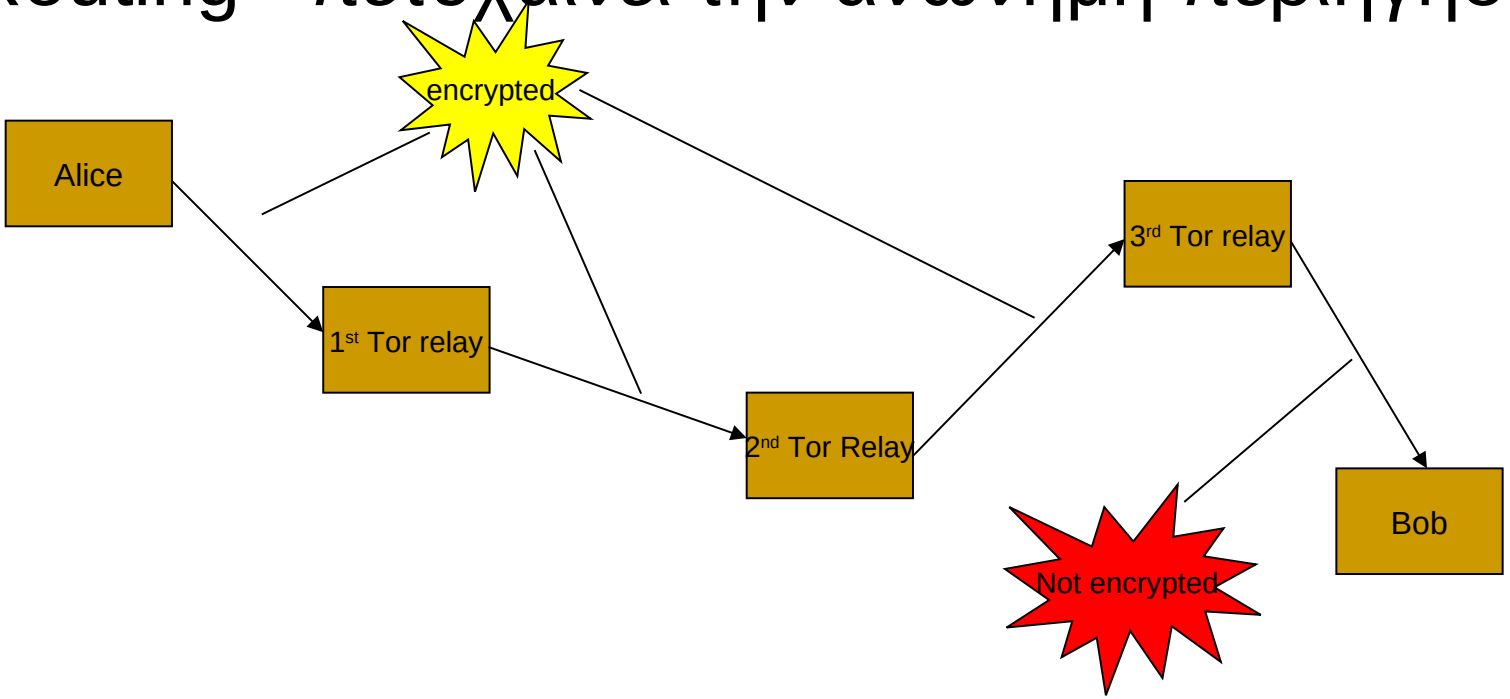
Ανώνυμη περιήγηση



Τα συστήματα αυτά, χρησιμοποιούν μία αλυσίδα από Proxy servers και κάθε μήνυμα *κρυπτογραφείται* καθώς μετακινείται από τον έναν Proxy στον άλλον.Το αποτέλεσμα είναι ο παραλήπτης να μην γνωρίζει τον αποστολέα.



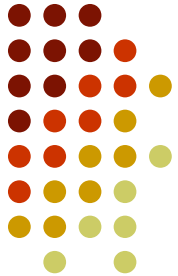
Το Tor project κάνοντας χρήση του «onion Routing» πετυχαίνει την ανώνημη περιήγηση.

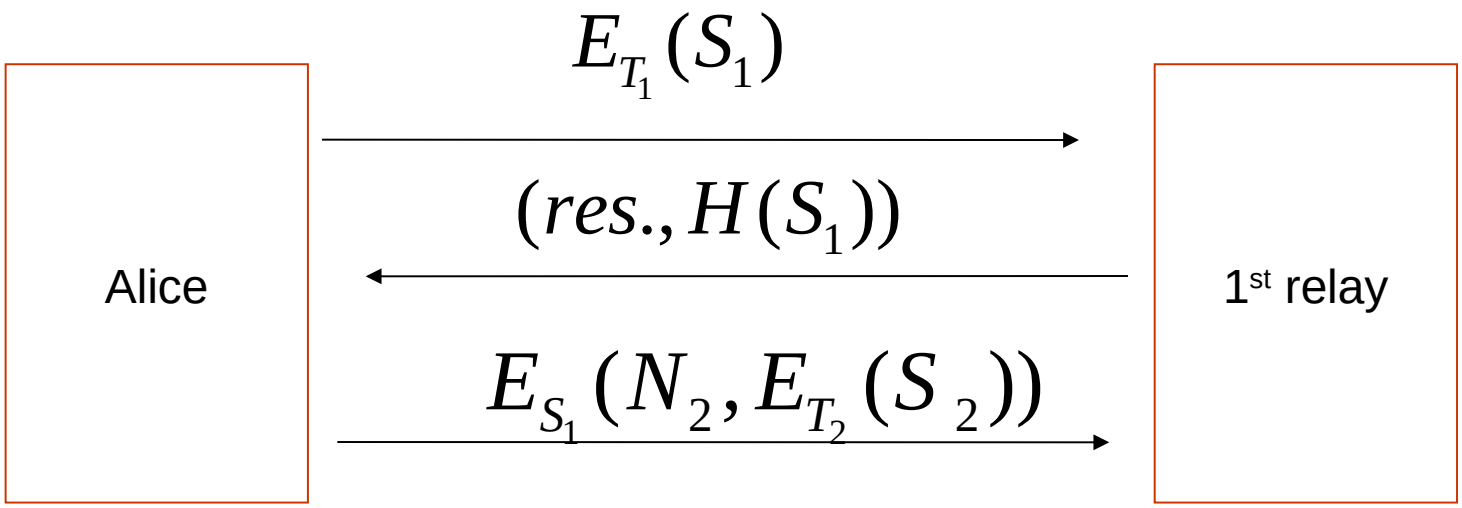


Ανώνυμη περιήγηση

- Ο τελευταίος Tor server μπορεί να δει τα δεδομένα που έχουμε στείλει, αλλά δεν ξέρει ποιος τα έστειλε. Ο Bob βλέπει τα δεδομένα που έστειλε η Alice αλλά δεν γνωρίζει ότι τα έστειλε αυτή.
- Ο 1ος Tor server βλέπει την IP της Alice αλλά όχι τα δεδομένα που στέλνει (διότι έχουν κρυπτογραφηθεί με τα δημ. Κλειδιά και των τριών nodes). Επίσης δεν βλέπει τον τελικό αποδέκτη του μηνύματος.
- Ο 2ος Tor server δεν ξέρει ούτε την IP της Alice ούτε τα δεδομένα που στέλνει.
- Ο 3ος (tor exit) βλέπει το μήνυμα που έστειλε η Alice στον Bob, αλλά δεν μπορεί να συνδέσει το μήνυμα αυτό με την Alice.

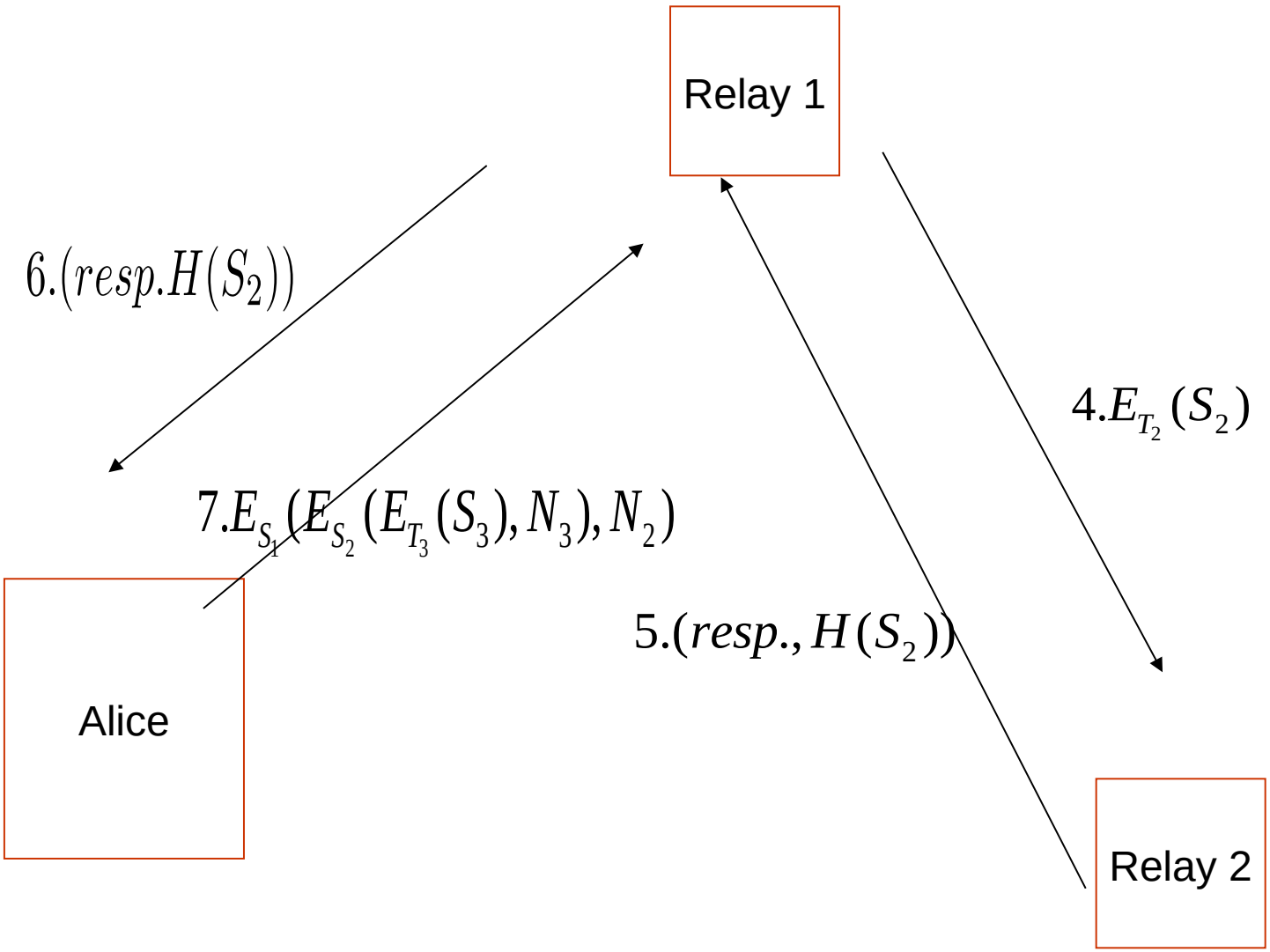
Στο πρώτο βήμα της επικοινωνίας της Alice με τον Bob η Alice με χρήση του Tor, φτιάχνει ένα δίκτυο (circuit) όπου με κάθε proxy server εκτελείται ένα πρωτόκολλο ανταλλαγής κλειδιού, όπου στο τέλος η Alice καταλήγει να έχει τρία δημόσια κλειδιά (onion public keys T1,T2,T3).



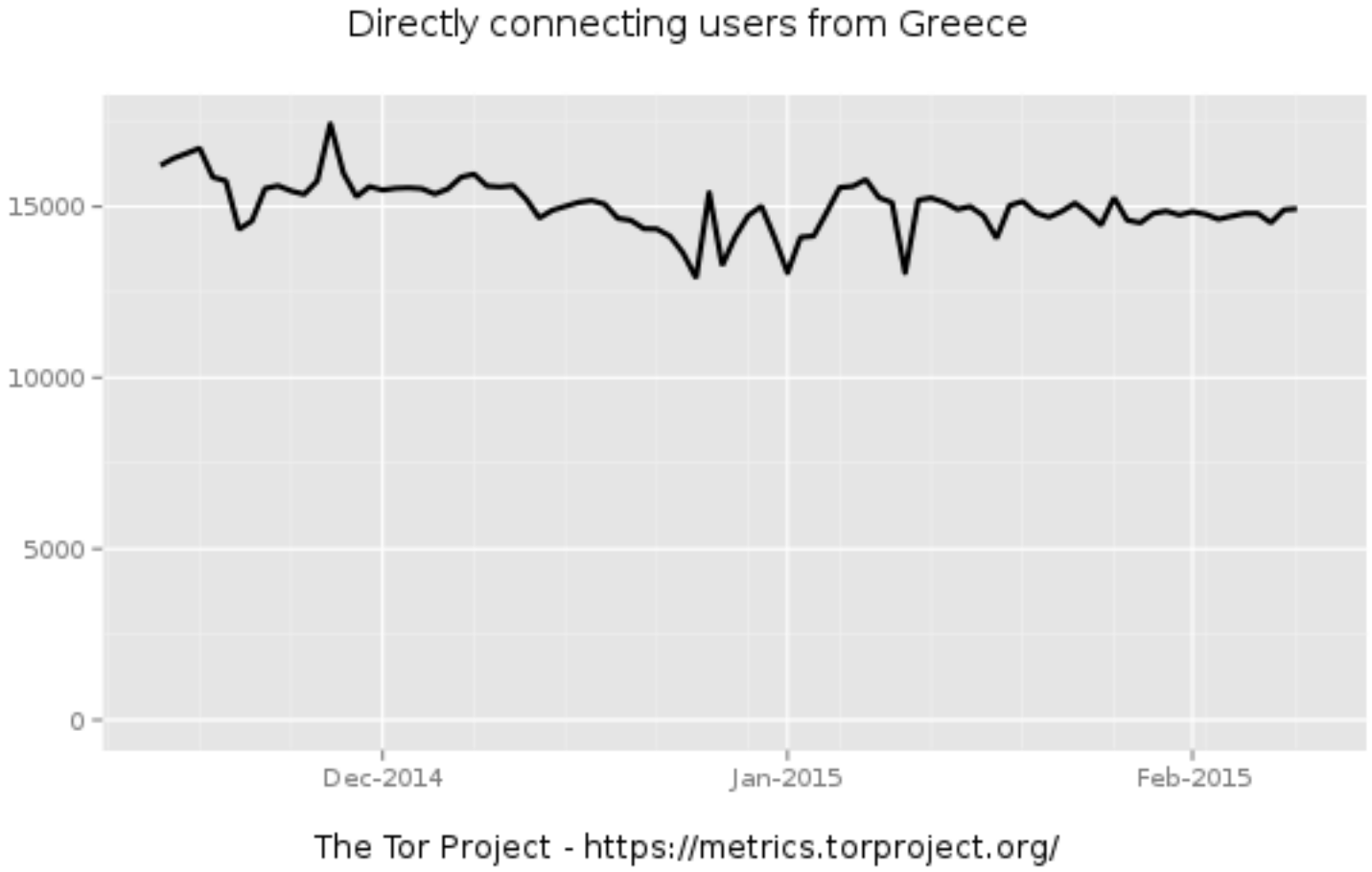


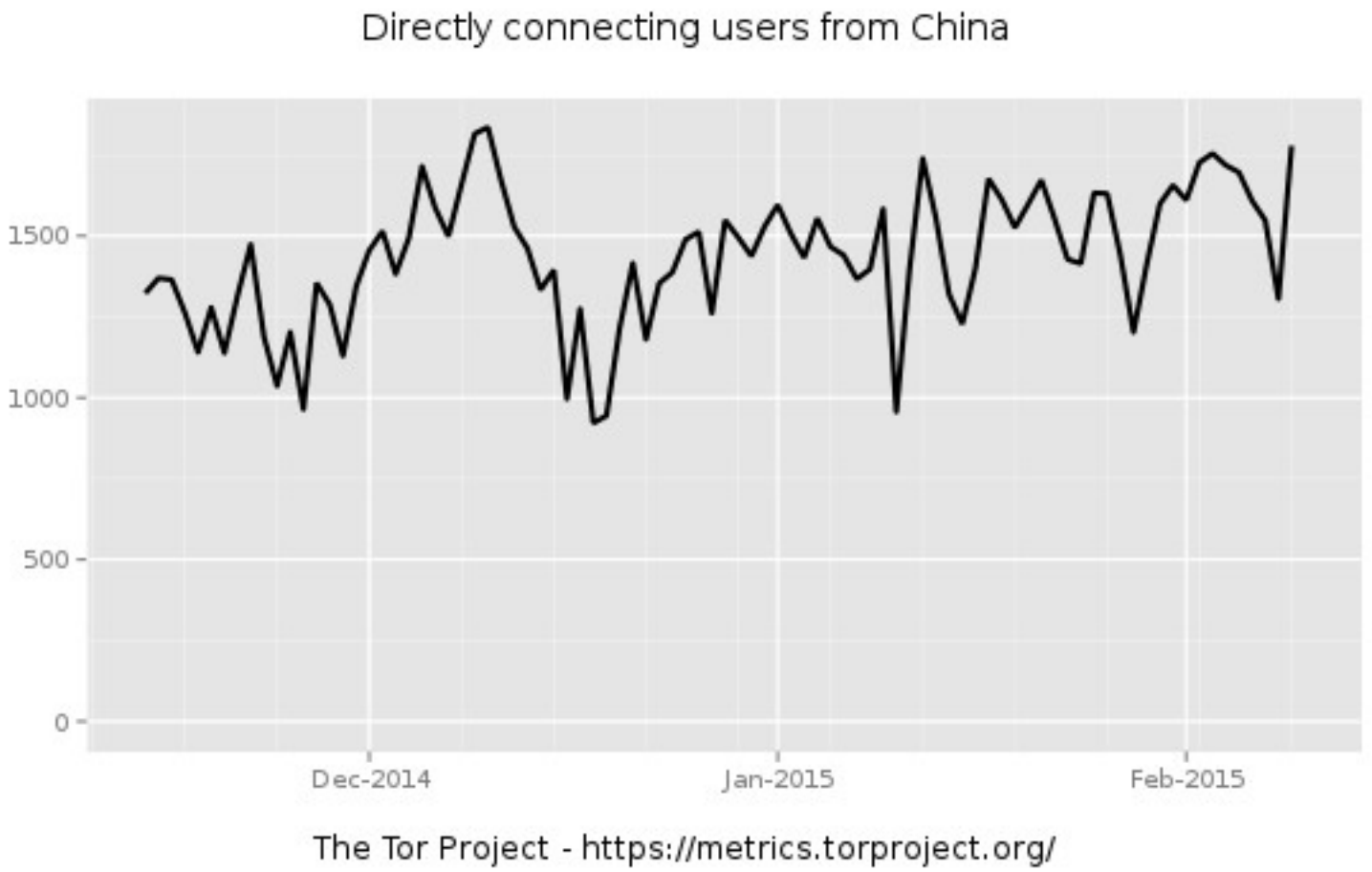
1ο Βήμα

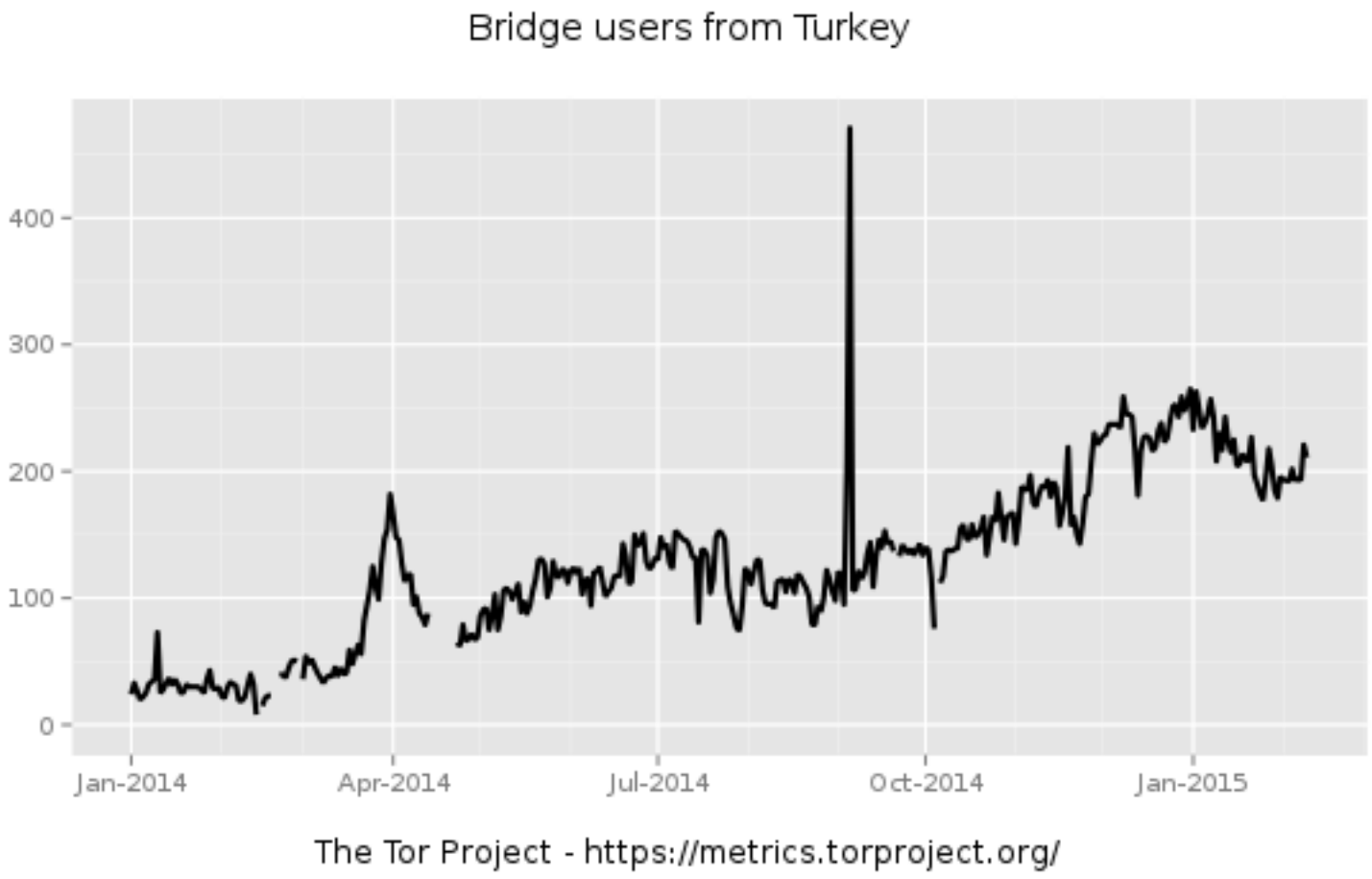
Στο βήμα 2 και 3 γίνεται η ίδια διαδικασία με τον 2ο και 3ο relay server.



4ο, 5ο, 6ο και 7ο βήμα της διαδικασίας.


Directly connecting users from Greece
15000
10000
5000
0
Dec-2014
Jan-2015
Feb-2015
The Tor Project - https://metrics.torproject.org/


Directly connecting users from China
1500
1000
500
0
Dec-2014
Jan-2015
Feb-2015
The Tor Project - https://metrics.torproject.org/


Bridge users from Turkey
400
300
200
100
0
Jan-2014
Apr-2014
Jul-2014
Oct-2014
Jan-2015
The Tor Project - https://metrics.torproject.org/

The reports describe "major problems" following users across the Tor network

No decrypt available for this PGP encrypted message

Source : http://www.theverge.com/2014/12/28/7458159/encryption-standards-the-nsa-cant-crack-pgp-tor-otr-snowden (13/2/2014)

https://citizenfourfilm.com/

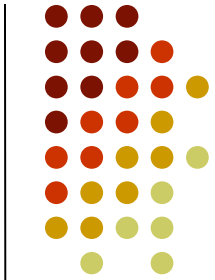
SSH-protocol

Αντικατέστησε το telnet. Χρησιμοποιει κρυπτογραφία δημοσίου κλειδιού. Για να πετύχει την αυθεντικοποίηση μεταξύ client-server. Κατόπιν χρησιμοποιεί συμμετρικη κρυπτογραφία (blowfish, AES) για κρυπτογράφηση δεδομένων. Η βασική του χρήση είναι να έχω ασφαλη απομακρυσμένη σύνδεση στην γραμμή-εντολών σε unix-type systems.

Η αυθεντικοποίηση γίνεται με το host key του server. Τη πρώτη φορά που συνδεόμαστε μας ζητάει ο server να αποδεχτούμε ένα κλειδι και επίσης μας δίνεται και το αποτύπωμα του κλειδιού. Πριν δεχτούμε το κλειδι, η σωστή διαδικασία είναι να επαληθεύσουμε το αποτύπωμα (π.χ. με απευθείας συνομιλία με τον sys-admin του server) Κατόπιν, κάθε φορά που θα συνδεόμαστε θα γίνεται αυτόματα έλεγχος αν το (public) host key είναι το σωστό.

Επίσης, μπορώ να χρησιμοποιήσω ssh-tunneling, π.χ. Όταν θέλει κάποιος να προσπεράσει ένα firewall ή για secure ftp.

Ψηφιακό χρήμα

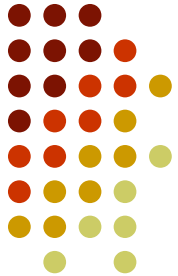


Το κανονικό χρήμα έχει δύο βασικές ιδιότητες.

1. Ο χρήστης είναι ανώνυμος στον αγοραστή
2. Εφόσον το κατέχει αυτόματα έχει δικαίωμα να το χρησιμοποιεί.

Οι πιστωτικές κάρτες ικανοποιούν μόνο την δεύτερη ιδιότητα. Το ψηφιακό νόμισμα bitcoin βασίζει την ασφάλεια του στις ψηφιακές υπογραφές

Bitcoin

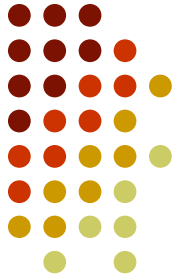


- Αποκεντρωμένο. Δεν χρειάζεται κάποια κεντρική αρχή η οποία παρέχει νομίσματα. Τα νομίσματα παράγονται εθελοντικά από pools, τα οποία καλούνται να λύσουν ένα μαθηματικό πρόβλημα (εύρεση αντιστροφης εικόνας στην sha256)
- Εμεις για να αποκτήσουμε bitcoins είτε συμμετέχουμε σε pools είτε κανουμε trading είτε τα αγοράζουμε απο ανταλλακτήρια.
- Μπορούμε να στείλουμε bitcoin σε οποιον θέλουμε (δινοντας μια μικρη προμηθεια στο δίκτυο), Η επαλήθευση της συναλλαγης γινεται σε περίπου δεκα λεπτά.
- Όλες οι συναλλαγες κρατουνται στο blockchain.
- Η διευθυνση μας δεν είναι human-meaningful αλλά το δημόσιο κλειδι μιας ψηφιακής υπογραφής.

Bitcoin

- Δεν ελέγχεται από κάποια κεντρικη αρχή.
- Στηρίζεται αποκλειστικά σε εθελοντές, που τρέχουν τα pools και παράγουν bitcoins.
- Η τεχνολογία blockchain που βασίζεται το bitcoin έχει και άλλες εφαρμογές.

PGP : Pretty Good Privacy



- Είναι ένα πρόγραμμα το οποίο υλοποιεί το πρωτόκολλο open PGP. Φτιάχτηκε αρχικά από τον προγραμματιστή – ακτιβιστή Phil Zimmermann. Στόχος του να μπορεί οποιοσδήποτε, να στέλνει ηλεκτρονικά μηνύματα (e-mails) με ασφάλεια. Σήμερα χρησιμοποιείται από παρα πολύ κόσμο που απαιτεί ασφάλεια στα e-mail του. Όπως για παράδειγμα δημοσιογράφους, στρατιωτικούς κλ.π.

PGP

- Το PGP είναι απαραίτητο σε δημοσιογράφους για να μιλούν με ασφάλεια με τις πηγές τους. Αλλά, και για τους απλούς πολίτες που θα επιθυμούσαν τα μηνυματα τους να είναι ασφαλή από τα αδιακριτα μάτια των sys-admins ή και από “διάφορους” που τυχαίνει να παρακολουθούν το κανάλι επικοινωνιας client-mail server.

E-voting

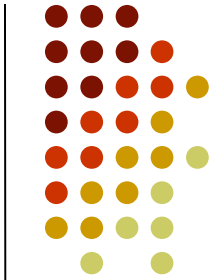
Σε αυτά τα συστήματα κάθε ηλεκτρονική ψήφος στέλνεται σε ένα κεντρικό server (voting center). Το κέντρο αυτό καταμετράει τις ψήφους χωρίς όμως να μπορεί να αναγνωρίσει την ταυτότητα του ατόμου που ψήφισε.

Instant Messengers

- Signal, Silent Phone

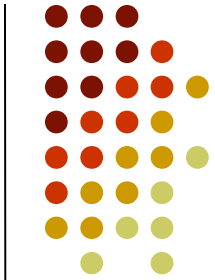
  Είναι text messengers σε android/desktop. Ο δε πρώτος υποστηρίζεται από τον ειδικό της κρυπτογραφίας Bruce Schneier καθώς και τον E.Snowden και L.Poitras. Ο δεύτερος είναι του Phil Zimmermann, τον προγραμματιστή του διάσημου PGP.

Zero-Knowledge proofs



Σε αυτά τα συστήματα κάποιος έχει αποδείξει ένα θεώρημα. Θέλει να πείσει ένα φίλο του ότι ξέρει την απόδειξη του θεωρήματος, χωρίς όμως να του τη δείξει.

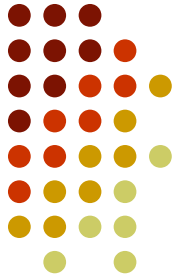
Post Quantum



Crypto based in lattices.

Ομομορφική κρυπτογράφηση

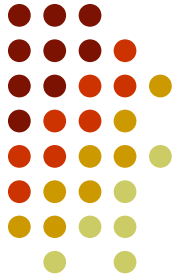
Το πρόβλημα της ομομορφικής κρυπτογράφησης



Στα ομομορφικά συστήματα ο Bob δεν γνωρίζει το ιδιωτικό κλειδί της Alice (ως συνήθως) επίσης γνωρίζει κάποια κρυπτογραφημένα μηνύματα c[1],c[2],..,c[k] και μία συνάρτηση f. Τότε, μπορεί να υπολογίσει την κρυπτογράφηση του μηνύματος f(m[1],m[2],…,m[k]). Φορμαλιστικά θέλουμε

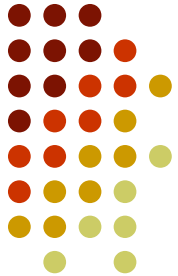
$$Dec(f(c_1, c_2, ..., c_n)) = f(m_1, m_2, ..., m_k)$$

Cloud Crypto

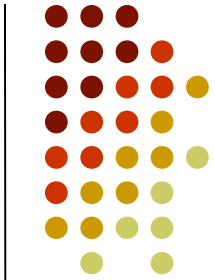


1ο σεναρίο. Έστω ότι έχετε έναν mail-provider που χρησιμοποιεί cloud. Έστω επίσης ότι όλα τα ηλ.μηνύματα σας είναι κρυπτογραφημένα με το δημόσιο κλειδί σας. Έστω ότι θέλετε να ψάξετε στα ηλ.μηνύματα για την λέξη : φόρος. Για να το κάνετε αυτό είτε πρέπει να αποκρυπτογραφήσετε ένα-ένα τα μηνυματα σας είτε να στείλετε το ιδιωτικό κλειδί σας στον παροχέα για να βρείτε τα μηνύματα που σας ενδιαφέρουν.

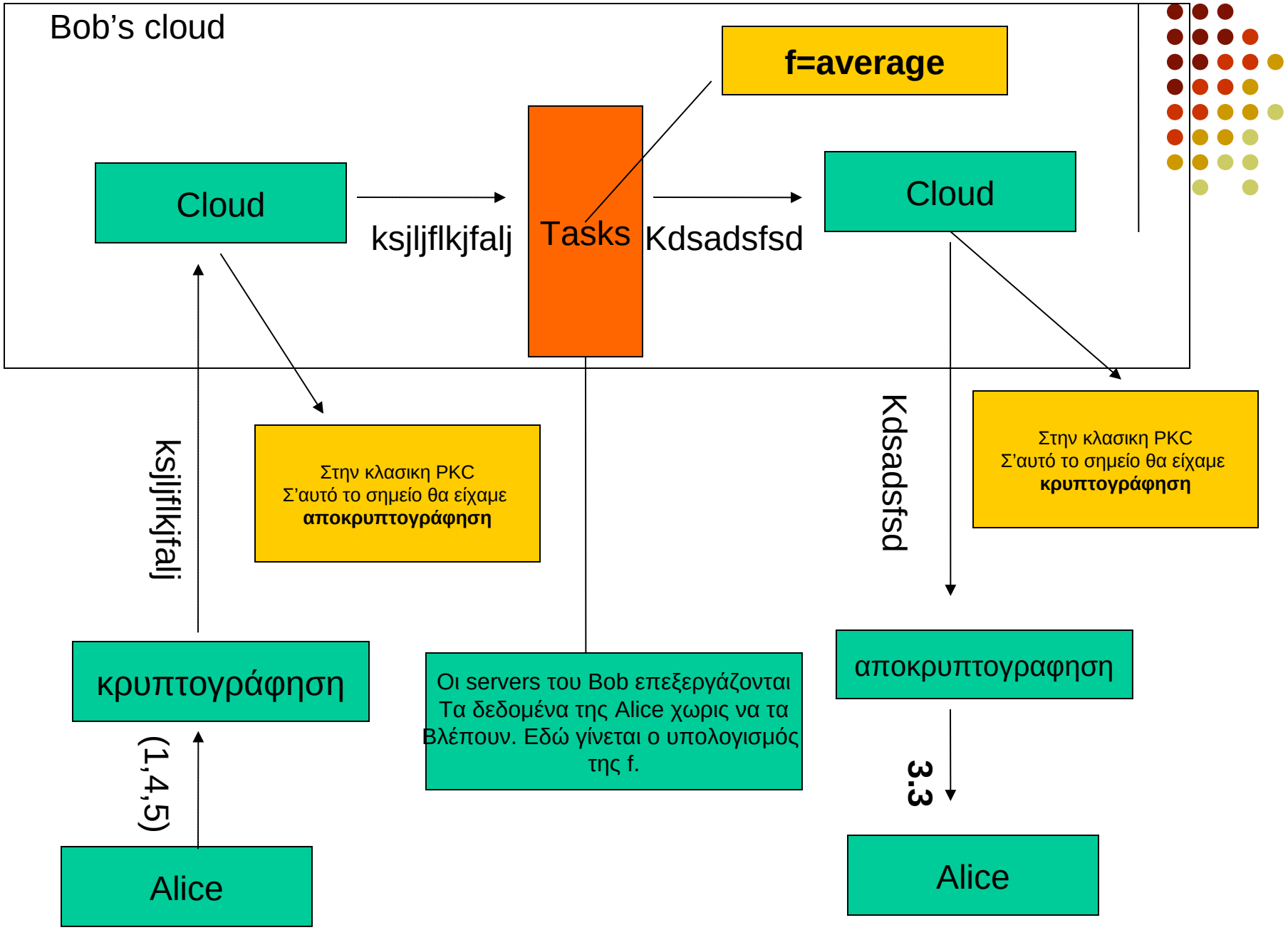
Cloud crypto



Μια λύση στο πρόβλημα θα ήταν να μπορείτε με κάποιο τρόπο να κάνετε κάποιες πραξεισστα κρυπτογραφημένα μηνύματα c[i] που να αντιστοιχούν σε κάποιες πράξεις στα m[i] χωρίς την χρήση του ιδιωτικού σας κλειδιού. Τα συστήματα αυτά ονομάζονται **F**ully **H**omomorphic **E**ncryption systems (FHE).



2ο σενάριο. Η Alice δουλευει σε μια εταιρεία που υλοποιεί συστήματα κρυπτογραφίας ενώ ο Bob σε εταιρεία cloud. Πάλι η Alice μπορεί να στέλνει κρυπτογραφημένα μηνύματα στον Bob με PK Crypto αλλά επίσης επιθυμεί κάποια μηνύματα να μην μπορεί να τα δει ο Bob. Δηλαδή θέλει να χρησιμοποιει τους διακομιστές του Bob να εκτελούν κάποιες εργασίες στα δεδομένα που στέλνει, αλλά ο Bob να μην μπορεί να δει τι κάνει η Alice.

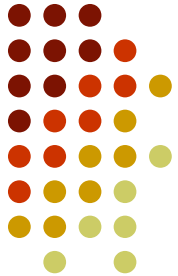

Bob's cloud
f=average
Cloud
ksjljflkjfalj
Tasks
Kdsadsfsd
Cloud
Στην κλασικη PKC
Σ'αυτό το σημείο θα είχαμε
αποκρυπτογράφηση
ksjljflkjfalj
Kdsadsfsd
Στην κλασικη PKC
Σ'αυτό το σημείο θα είχαμε
κρυπτογράφηση
κρυπτογράφηση
Οι servers του Bob επεξεργάζονται
Τα δεδομένα της Alice χωρις να τα
Βλέπουν. Εδώ γίνεται ο υπολογισμός
της f.
αποκρυπτογραφηση
(1,4,5)
3.3
Alice
Alice

Rivest-Shamir (again) and Dertouzos!

(https://en.wikipedia.org/wiki/Michael_Dertouzos)

Η πρωτη ιδέα της ομομορφικής κρυπτογράφησης ήταν των Rivest-Shamir-Derouzos το 1978. Το πρώτο FHE δόθηκε το 2009 από τον Gentry. Το σύστημα του Gentry χρησιμοποιεί πιθανοτικη κρυπτογράφηση εισάγοντας την έννοια του *noise computation.* Κωδικοποιεί το προβλημά του σε Lattice. Σε κάθε σημείο εισάγει θόρυβο. Τα σημεία που δημιουργουνται είναι το κρυπτογραφημένο μήνυμα. Κατόπιν γίνονται οι πράξεις επί των νέων σημείων. Η αποκρυπτογράφηση γίνεται με φιλτράρισμα του θορύβου. Αν ο θόρυβος ξεπεράσει ένα όριο τότε η αποκρυπτογράφηση επαναλαμβάνεται.

Lightweight Crypto



Τεχνολογίες όπως RFID(passive), sensors, coprocessors, smart clothes κ.λ.π. και γενικά όπου έχω λίγη μνήμη και υπολογιστική δύναμη (συνήθως την μετράμε με gate-equivalents, π.χ. ο AES-128 χρειάζεται 3400GE) είναι δύσκολο εώς αδύνατο να υλοποιήσουμε κρυπτογραφία συμμετρική και ακόμη πιο δύσκολα δημοσίου κλειδιού. Τα RFID χρησιμοποιούνται ήδη ως ιατρικά εμφυτευματα, στα διαβατήρια, στις πιστωτικές, στα διόδια, στα τραπεζικά νομίσματα, σαν barcodes κ.α.

GE-crypto primitives

Μερικά παραδείγματα κρυπτοσυστημάτων και τα ισοδύναμα τους σε GE για να υλοποιηθούν σε επίπεδο πυλών.

Ένα RFID διαθέτει 10000GE και για κρυπτογραφία είναι διαθέσιμες περίπου 3000GE.

Primitive	G.E.
AES-128 (sym.)	3400
NTRUe (pkey)	2850
DES (sym.)	2309
EEC-112 (pkey)	10113
PRESENT-80 (sym.)	1075
WIPR (pkey)	5700
SEA (sym.)	449
SHA256	10800
Trivium	2600
md5	8400

Ερωτήσεις

- Εσείς ως νέοι επιστήμονες της πληροφορικής πιστεύετε ότι έχετε τις απαραίτητες γνώσεις να κατανοήσετε τους κινδύνους στο διαδίκτυο;
- Πως θα σχολιάζατε την θέση : *I have nothing to hide.*

- **Στοιχεία από πιθανότητες**
- **Παράδοξο των γενεθλίων**
- **Τέλεια ασφάλεια κατά Shannon**

Ας είναι $U = \{0,1\}^n$ ένα πεπερασμένο σύνολο.

Ορισμός. Μία κατανομή πιθανότητας είναι μια συνάρτηση P:U→[0,1] τ.ω.

$$\sum_{x \in U} P(x) = 1$$

Για παράδειγμα η ομοιόμορφη κατανομή :

$$\forall x \in U, P(x) = \frac{1}{|U|}$$

Ενώ διάνυσμα της κατανομής ονομάζω π.χ. για την περίπτωση n=2 το διάνυσμα P(0,0),P(1,0),P(0,1),P(1,1)).

Ενδεχόμενο ονομάζω κάθε υποσύνολο A του U.

Παρατηρήστε ότι P(U)=1.

Παράδειγμα

Ας είναι $U = \{0,1\}^4$

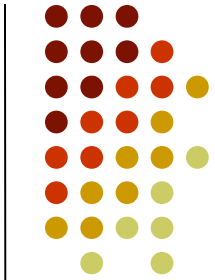
Βρείτε την πιθανότητα του ενδεχομένους Α που τα δύο τελευταία λιγότερο σημαντικά ψηφία του είναι το 10. Δηλαδή,

$$A = \{x \in U : lsb_2(x) = 10\}$$

Υποθέτουμε ότι η επιλογή των ψηφίων γίνεται με τυχαίο τρόπο.

Λύση. Το |U|=2^4=16. Για τα δύο πιο σημαντικά ψηφία, εφόσον είναι δυαδικά ψηφία, έχουμε 2^2=4 δυνατότητες. Εφόσον, η επιλογή γίνεται τυχαία (ομοιόμορφα)

P(A)=4/16=1/4

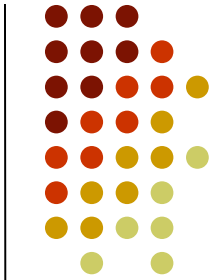


Ονομάζουμε τυχαία μεταβλητή X μια συνάρτηση από τον δειγματοχώρο U→V, όπου V ένα υποσύνολο του R. Δηλ. Οι τ.μ. είναι πραγματικές συναρτήσεις, αλλά υπάρχουν και τ.μ. που μπορούν να έχουν τιμές στο σύνολο {True, False}, σε πίνακες, σε ακολουθίες κ.λπ.

Παράδειγμα. Αν

$$X:\{0,1\}^n \to \{0,1\} \text{ με } X(z)=lsb(z), \text{ δηλαδή αν } z=101...01, \text{ τότε}$$

$$X(z)=1. \text{ Έχουμε } P(X=1)=\frac{1}{2}, P(X=0)=\frac{1}{2}.$$



Ας είναι $U = \{0,1\}^n$. Ονομάζουμε ομοιόμορφη τ.μ. r (και συμβολίζουμε $r \xleftarrow{R} U$), την τ.μ. που ικανοποιεί την $P(r = a) = \frac{1}{|U|} = \frac{1}{2^n} \quad \forall a \in U.$

Παράδειγμα. Έστω $r_1, r_2 \xleftarrow{R} U = \{0,1\}^3$

με $r_1 : U \to \{0,1\},$ με $r_1(abc) = a$ και

$r_3 : U \to \{0,1\},$ με $r_3(abc) = c.$

και $X(z) = r_1(z) + r_3(z).$

Τότε $P(X = 2) = 1/4$

Ένωση και τομή ενδεχομένων

Ισχύει $P(A \cup B) \leq P(A) + P(B)$

Ορισμός. Λέμε ότι τα ενδεχόμενα Α,Β, είναι ανεξάρτητα μεταξύ τους αν

$$P(A \cap B) = P(A)P(B)$$

Επίσης δύο ενδεχόμενα ονομάζονται ξένα μεταξύ τους αν $A \cap B = \varnothing$

Σ'αυτή την περίπτωση ισχύει $P(A \cup B) = P(A) + P(B)$

Δεσμευμένη πιθανότητα

Αν γνωρίζουμε ότι έχει συμβεί κάποιο γεγονός, π.χ. το Β, και θέλουμε να υπολογισουμε την πιθανότητα να συμβεί ένα γεγονός Α, τότε μιλάμε για **δεσμευμένη πιθανότητα** του Α όταν έχει συμβεί το Β και γράφουμε P(A|B)

Ορισμός 1. Αν $B \neq \emptyset$

τότε $P(A|B) = \dfrac{P(A \cap B)}{P(B)}$

Αν όλα τα αποτελέσματα είναι ισοπίθανα

$$P(A|B) = \frac{|A \cap B|}{|B|}$$

Πρόβλημα 1. Ρίχνουμε ένα αμερόληπτο κέρμα τρεις φορές. Ποια είναι η πιθανότητα P(A|B) όταν

Α={οι κορώνες είναι περισσότερες από τα γράμματα}

Β={να έρθει στην 1η ρίψη γράμματα}

Γ={να έρθει στην 1η ρίψη κορώνα}

Λύση. Υπολογίζουμε το P(B) = ½

Κατόπιν, υπολογίζουμε την $P(A \cap B) = 1/8$

Άρα,

$$P(A|B) = \frac{1/8}{1/2} = \frac{2}{8} = \frac{1}{4}$$

Ενώ,

$$P(A|\Gamma) = \frac{P(A \cap \Gamma)}{P(\Gamma)} = \frac{3/8}{4/8} = \frac{3}{4}$$

Κανόνας του Bayes

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

Όπου A,B ενδεχόμενα με P(B) διάφορο του μηδενός.

$P(A)$ η πιθανότητα να παρατηρηθεί το ενδεχόμενο A

$P(B)$ η πιθανότητα να παρατηρηθεί το ενδεχόμενο B

Αυτές οι πιθανότητες ονομάζονται και οριακές πιθανότητες (marginal probabilities)

Πιθανοτικοί Αλγόριθμοι

Ο ντετερμινιστικός αλγόριθμος για μια είσοδο m δίνει πάντα το ίδιο αποτέλεσμα.

Ο πιθανοτικός αλγόριθμος Α εξαρτάται και από μια τυχαία μεταβλητή r.

Είναι της μορφής $z \leftarrow A(m;r)$

Άρα ένα πιθανοτικός αλγόριθμος ορίζει μια τ.μ. πάνω στο σύνολο των αποτελεσμάτων.

XOR (αποκλειστική διάζευξη)

Ερώτηση : αν $z \in \{0,1\}^n$

τότε $z \oplus z = ?$

Θεώρημα. Αν X τ.μ. πάνω στο $U = \{0,1\}^n$ και Y ομοιόμορφη τ.μ. πάνω στο U ανεξάρτητη απ'την X, τότε η τ.μ. $Z = X \oplus Y$ είναι ομοιόμορφη τ.μ. πάνω στο U.

Απόδειξη. (για n=1). Αρκεί ν.α.ο.

$$P[Z=0]=1/2.$$

Οι πίνακες κατανομής των τ.μ. X,Y,Z είναι

X	p
0	P[0]
1	P[1]

Y	p
0	1/2
1	1/2

X	Y	p
0	0	P[0]/2
0	1	P[0]/2
1	0	P[1]/2
1	1	P[1]/2

Ισχύει $P[z=0]=P[(X,Y)=(0,0)\ \text{ή}\ (X,Y)=(1,1)]=$

$$=P[(X,Y)=(0,0)]+P[(X,Y)=(1,1)]=$$

$$=\frac{p_0}{2}+\frac{p_1}{2}=\frac{p_0+p_1}{2}=\frac{1}{2}\ \text{ο.ε.δ.}$$

Τι είναι κρυπτοσύστημα;
(Μαθηματικός ορισμός)

Ένα κρυπτοσύστημα επί της τριάδας (K, M, C)
Είναι ένα ζευγάρι «αποδοτικών» αλγορίθμων (E,D) και ένας αλγόριθμος Gen που παράγει τα ιδιωτικά κλειδια, τέτοιοι ώστε

$$E : K \times M \to C,\ D : K \times C \to M$$

$$E(k,m) = c,\ D(k, E(k,m)) = m,\ \forall (k,m) \in K \times M$$

E: είναι συχνά πιθανοτικός αλγόριθμος,

D: ντετερμινιστικός αλγόριθμος

One time pad

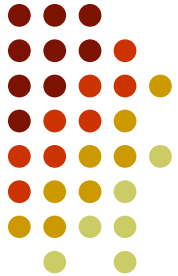
Πρώτος ο Frank Miler ανακάλυψε τον OTP. Επίσης το 1917 ανακαλύφθηκε ανεξάρτητα από τον Gilbert Vernam (με την πρόσθεση mod 2). Η σωστή του χρήση όμως δόθηκε από τον Joseph Mauborgne . Η λάθος χρήση αυτού του συστήματος στο πρόγραμμα Venona, επέτρεψε την αποκρυπτογράφηση περίπου 3000 μηνυμάτων των σοβιετικών, την περίοδο του δεύτερου Παγκοσμίου Πολέμου.

Number stations

Οι σταθμοί αριθμών είναι ένα τύπος ραδιοφωνικών σταθμών (shortwave radio stations) που εκπέμπουν σε συχνότητες μεταξύ 1.3 και 30 MHz (λίγο πάνω από τα μεσαία AM). Είναι ικανοί να μεταδώσουν μηνύματα σε μεγάλες αποστάσεις, επειδή ανακλώνται στην ιονόσφαιρα. Οι σταθμοί αριθμών χρησιμοποιούν αυτές τις συχνότητες για να στείλουν κρυπτογραφημένα μηνύματα σε απομακρυσμένους πράκτορες κάνοντας χρήση του OTP.

[https://en.wikipedia.org/wiki/Numbers_station]

One Time Pad (OTP)



Ο OTP αποτελεί το μοναδικό παράδειγμα ασφαλούς κρυπτοσυστήματος. Εδώ έχουμε

$$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$$

Το κλειδί έχει μήκος όσο το μήκος του μηνύματος. Ο αλγόριθμος Gen επιστρέφει κλειδιά μήκους n, που επιλέγονται ομοιόμορφα από το

$$\{0,1\}^n$$

One Time Pad

Για να κρυπτογραφήσω με τον OTP κάνω XOR το μήνυμα με το κλειδί (bit με bit).

Επομένως, $E(k,m) = c = k \oplus m$

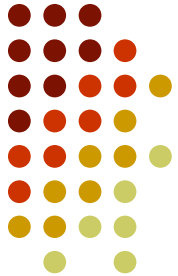
Ενώ η αποκρυπτογράφηση είναι $D(k,c) = k \oplus c$

Ισχύει D(k,E(k,m))=m;

One Time Pad

Ερώτηση. Αν γνωρίζουμε το μήνυμα m και το κρυπτομήνυμα c, μπορούμε να βρούμε το κλειδί k;

One Time Pad



Ο OTP έχει πολύ «γρήγορη» κρυπτογράφηση και αποκρυπτογράφηση. Παρόλα αυτά έχει μεγάλο μήκος κλειδιού και αυτό τον κάνει μη πρακτικό. Το ερώτημα είναι, αν είναι αρκετά ασφαλής για να τον χρησιμοποιήσω;

One Time Pad

Στο ερώτημα αυτό απάντησε ο Shannon.

Απόδειξε το 1946, ότι ο OTP έχει «τέλεια ασφάλεια».

Τέλεια ασφάλεια σημαίνει ότι αν κάποιος έχει το κρυπτομήνυμα c, αυτό δεν του παρέχει καμιά πληροφορία για το αρχικό μήνυμα m, και αυτό συμβαίνει για κάθε m,c.

Πριν ασχοληθούμε με αυτόν τον ορισμό, πρέπει να καταλάβουμε τι σημαίνει να είναι ασφαλές ένα σύστημα.

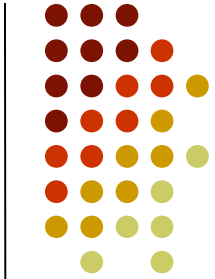
Τι σημαίνει ένα κρυπτοσύστημα είναι ασφαλές;

Threat model for encryption : Ciphertext only attack.

Υποθέτουμε ότι η Alice και ο Bob έχουν ένα κοινό κλειδί k που έχει παραχθεί από τον αλγόριθμο Gen. Η Alice στέλνει το μήνυμα c=E(k,m) και η Eve το κλέβει μέσα από το κανάλι επικοινωνίας.

Ασφαλές θα μπορούσε να ήταν το κρυπτοσυστημα μας αν :

1. είναι αδύνατον η Eve να μπορεί να βρει το κλειδί k; ή
2. είναι αδύνατον η Eve να μπορεί να βρει το m από το c; ή
3. είναι αδύνατον η Eve να μπορεί να βρει έναν χαρακτήρα του m;

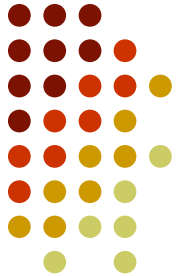


Το 1 δεν είναι καλός ορισμός ασφάλειας. Για παράδειγμα, θεωρείστε το κρυπτοσύστημα E(k,m)=m για κάθε m. Παρότι είναι δύσκολο να βρεί η Eve το κλειδί, είναι πολύ εύκολο να βρει το μήνυμα m.

Το 2 επίσης δεν είναι καλός ορισμός ασφάλειας, αλλά είναι καλύτερος από τον ορισμό 1. Ας πάρουμε για παράδειγμα ένα κρυπτοσύστημα στο οποίο η Eve μπορεί να μαθαίνει το 80% του μηνύματος m. Σύμφωνα με τον ορισμό 2 αυτό το σύστημα είναι ασφαλές (αφου η Eve δεν μαθαίνει όλο το μηνυμα). Φυσικά ένα τέτοιο σύστημα δεν μπορεί να θεωρηθεί ασφαλές.

Επίσης το 3 δεν είναι καλός ορισμός ασφάλειας αλλά είναι καλύτερος από τον 2. Ας θεωρήσουμε ένα κρυπτοσύστημα όπου η Eve δεν μαθαίνει κανένα χαρακτήρα του μηνύματος m αλλα μπορεί να μάθει άλλες πληροφορίες για το μήνυμα m. Για παράδειγμα, αν η Alice στέλνει λεφτά στον Bob, π.χ. 1000E. Η Eve δεν μπορεί να μάθει το ποσό, αλλά για παράδειγμα μπορεί να μάθει ότι είναι περισσότερα από 500E. Ένα τέτοιο σύστημα επίσης δεν μπορεί να θεωρηθεί ασφαλές.

Ο σωστός ορισμός : Ανεξάρτητα από την “προηγούμενη” γνώση που έχει η Eve για το μήνυμα **m**, η Eve κλέβοντας το κρυπτομήνυμα **c**, δεν αποκτά κάποια επιπλέον πληροφορία για το μήνυμα **m**.



Ο ορισμός αυτός δόθηκε από τον Cloude Shannon το 1945, στην εργασία του A Mathematical Theory of Cryptography.

Για να εκφράσουμε μαθηματικά τον προηγούμενο ορισμό χρειαζόμαστε την έννοια της δεσμευμένης πιθανότητας. Έστω $(\mathcal{M}, \mathcal{C}, \mathcal{K})$ ο χώρος μηνυμάτων, κρυπτογραφημένων μηνυμάτων και κλειδιών αντίστοιχα και (Gen,E,D) οι αλγόριθμοι παραγωγής κλειδιών, κρυπτογράφησης και αποκρυπτογράφησης, αντίστοιχα.

‘Εστω
- K η τυχαία μεταβλητή που δηλώνει το κλειδί,
- M η τ.μ. που δηλώνει το μήνυμα και
- C η τ.μ. που δηλώνει το κρυπτογραφημένο μήνυμα.

Για παράδειγμα, ο αλγόριθμος Gen ορίζει μια κατανομή πιθανότητας επί του συνόλου $\mathcal{K}$

$$Pr(K = k) = Pr(Gen \text{ produces k})$$

Μια λογική υπόθεση που κάνουμε είναι η εξής :
Οι τ.μ. M και K είναι ανεξάρτητες.
Δηλαδή, το μήνυμα που λαμβάνει ο Bob, δεν εξαρτάται από το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση του.

Επομένως αν έχουμε ένα συγκεκριμένο κρυπτοσύστημα, θα έχουμε και την κατανόμη της τ.μ. M επί του χώρου μηνυμάτων καθώς
και την κατανομή της τ.μ. K επί του χώρου κλειδιών.

Εκτελούμε το εξής πείραμα:
1. Διαλέγουμε ένα μήνυμα m σύμφωνα με την κατανομή της τ.μ. M
2. Παράγουμε ένα κλειδί k σύμφωνα με την κατανομή της K
3. Υπολογίζουμε το c = E(k,m)

Αυτό το πείραμα ορίζει μια νέα τ.μ., την ονομάζουμε C, επί του χώρου $\mathcal{C}$

Τελικά, ο ορισμός της τέλειας ασφάλειας (perfect security), μπορεί να γραφτεί ως εξής :

1ος ορισμός τέλειας ασφάλειας

Για οποιαδήποτε κατανομή πιθανότητας που ακολουθεί η τ.μ. M και για κάθε μήνυμα m και κρυπτογραφημένο μήνυμα c (με Pr[C=c]>0), ισχύει

$$Pr(M = m|C = c) = Pr(M = m)$$

A posteriori probability
η πιθανότητα M=m όταν γνωρίζουμε το κρυπτομήνυμα c

A priori probability
Η πιθανότητα το M=m

Δηλ. η γνώση του c δεν παρέχει κάποια επιπλέον πληροφορία για το μήνυμα m.

Μια συνέπεια του προηγούμενου ορισμού είναι το παρακάτω θεώρημα.

Θεώρημα. Ικανή και αναγκαία συνθήκη για να έχει ένα κρυπτοσύστημα τέλεια ασφάλεια είναι :

$$Pr(C = c|M = m) = Pr(C = c)$$

για όλα τα μηνύματα m και κρυπτομηνύματα c.

Απόδειξη. Από τον ορισμό 1 και το θεώρημα του Bayes έχουμε,

$$Pr[M = m|C = c] = \frac{Pr[C = c|M = m] \cdot Pr[M = m]}{Pr[C = c]}$$

Εφόσον το σύστημα έχει τέλεια ασφάλεια $Pr[M = m|C = c] = Pr[M = m]$

Οπότε το ζητούμενο προκύπτει άμεσα. Ο.ε.δ.

Δηλαδή, η συνολική πιθανότητα των κλειδιών που μετασχηματίζουν το μήνυμα m[0] στο c ισούται με την συνολική πιθανότητα των κλειδιών που μετασχηματίζουν το m[1] στο c και αυτό ισχύει για κάθε m[0],m[1] και c.

Υπάρχει ένας ακόμη ορισμός της τέλειας ασφάλεια που δεν εμπλέκει α posteriori και a priori πιθανότητες. Ο προηγούμενος ορισμό δόθηκε από τον C. Shannon το 1946 (αλλά το άρθρο του δημοσιεύτηκε το 1949).

2ος ορισμός τέλειας ασφάλειας

Έστω (E,D,Gen.) ένα κρυπτοσύστημα επί των συνόλων $(\mathcal{M},\mathcal{C},\mathcal{K})$. Λέμε ότι το προηγούμενο κρυπτοσύστημα έχει τέλεια ασφάλεια αν-ν για κάθε $m_0,m_1 \in \mathcal{M}$ και για κάθε $c \in \mathcal{C}$,

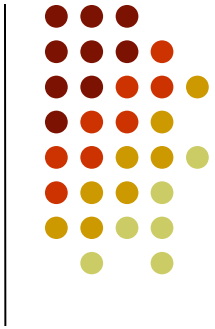
$$Pr(k \xleftarrow{K} \mathcal{K} : E(k,m_0) = c) = Pr(k \xleftarrow{K} \mathcal{K} : E(k,m_1) = c)$$

Θεώρημα ισοδυναμίας

Χωρίς απόδειξη δίνουμε το παρακάτω.

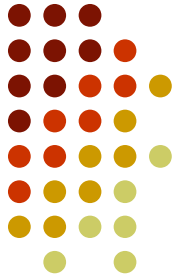
Οι ορισμοί 1 και 2 είναι ισοδύναμοι

Για την απόδειξη μπορείτε να δείτε [εδώ]



- Δηλαδή αν η Εύα “κλέψει” το c, τότε δεν έχει ιδέα αν αυτό προήλθε από το m[0] ή από το m[1].

Τέλεια ασφάλεια του One Time Pad



1ο Θεώρημα του Shannon.

Ο OTP έχει τέλεια ασφάλεια.

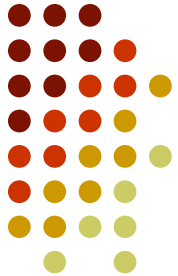
Απόδειξη. Αρκεί ν.α.ο. για κάθε με **M** και σε **C** η πιθανότητα P(E(k,m)=c) (καθώς το k διατρέχει όλα τα κλειδιά στο **K**) είναι ανεξάρτητη από το m. Πράγματι, τότε ικανοποιείται ο ορισμός Τ.Α. του Shannon.

Ισχύει $P[E(k,m)=c] = \dfrac{\#\{k \in K : E(k,m)=c\}}{\#K}$.

Αλλά $\#\{k \in K : E(k,m)=c\} = 1$. Πράγματι η εξίσωση $k \oplus m = c$, έχει μοναδική λύση ως προς k, την $k = m \oplus c$.

Άρα $P[E(k,m)=c] = \dfrac{1}{2^n}$ (σταθερά ανέξαρτητη από το m).

One Time Pad



Παρόλα αυτά ο OTP δεν χρησιμοποιείται στην **πράξη**. Υπενθυμίζουμε ότι η βασική αδυναμία του OTP είναι ότι τα κλειδιά πρέπει να έχουν μήκος όσο το μήκος του μηνύματος.

Ερώτηση. Μήπως υπάρχουν κρυπτοσυστήματα που έχουν Τ.Α. αλλά μικρά κλειδιά;

One Time Pad

2ο Θεώρημα (Shannon).

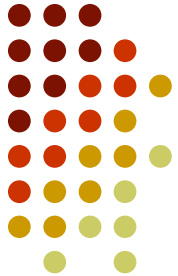
Αν ένα κρυπτοσύστημα έχει Τ.Α. τότε

μήκος του κλειδιού≥μήκος του μηνύματος

Πως μπορούμε να κάνουμε πρακτικό τον OTP;

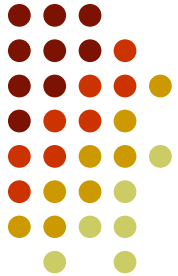
Θα πρέπει να εισάγουμε τις γεννήτριες ψευδοτυχαίων αριθμών (PRG). Τα νέα συστήματα που θα προκύψουν θα τα ονομάσουμε κρυπτοσυστήματα ροής.

Σημασιολογικά Ασφαλές κρυπτοσύστημα



Ένας πιο ρεαλιστικός ορισμός ασφάλειας είναι η σημασιολογική ασφάλεια (SS-Semantic Security). Θα μπορούσαμε να ονμάσουμε αυτό το επίπεδο ασφάλειας : πρακτικά τέλεια ασφάλεια. Η διαφορά με την τέλεια ασφάλεια είναι ότι εδώ η Eve έχει "πολυωνυμική δύναμη". Θυμηθείτε ότι στον ορισμό της τέλειας ασφάλειας, δεν έγινει κάποια υπόθεση για τις δυνατότητες της Eve. Στον ορισμό της σημασιολογικής ασφάλειας υποθέτουμε ότι η Eve έχει στην κατοχή της πολυωνυμική υπολογιστική δυνατότητα και όχι "άπειρη" όπως στον ορισμό της τέλειας ασφάλειας.

Η ιδέα της σημασιολογικής ασφάλειας δόθηκε πρώτη φόρα από την **Shafi Goldwasser** και τον **Silvio Micali**, το 1984, στην εργασία τους :
Probabilistic encryption & how to play mental poker keeping secret all partial information.



Σε αυτή την εργασία εκτός του ορισμού της σημασιολογικής ασφάλειας, δίνεται και ο ορισμός της "partial information". Επίσης δίνεται έμφαση στην χρήση της πιθανοτικής κρυπτογράφησης έναντι της ντετερμενιστικής.

Ας δούμε πως όρισαν την έννοια της "μερικής πληροφορίας".
Ορισμός. Έστω $f : \mathcal{M} \to \{0,1\}$ μια αποδοτική συνάρτηση. Αν η Eve γνωρίζει το c=E(k,m) και μπορεί να υπολογίσει το f(m), λέμε ότι τότε έχει μια μερική πληροφορία για το m.

Όπως έχουμε ήδη δει, επί του χώρου μηνυμάτων υπάρχει μια κατανομή P. Υποθέτουμε ότι η πιθανότητα η συνάρτηση f να πάρει την τιμή 1(true) είναι p>0.5 ως προς την κατανομή P.
Ορισμός. Η Eve έχει πλεονέκτημα ε>0 στον υπολογισμό της συνάρτησης f, αν η πιθανότητα Pr{f(m)=1, όταν γνωρίζει το c}>p+ε.
Ορισμός (σημασιολογική ασφάλεια).
Αν η Eve δεν έχει πλεονέκτημα ε, λέμε ότι το σύστημα είναι σημασιολογικά ασφαλές.

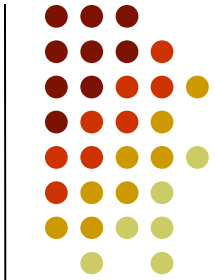
Για να αποδείξουμε ότι ένα κρυπτοσυστήμα δεν είναι σημασιολογικά ασφαλές, αρκεί να βρούμε μια f (την συναρτηση αυτή την λέμε και predicate) επί του χώρου μηνυμάτων, ώστε να μπορεί να υπολογιστεί με “μεγάλη” πιθανότητα η πιθανότητα του ενδεχομένους {f(m)=1}
επί ενός (τυχαίου) μηνύματος m εάν έχουμε το κρυπτογραφημένο μήνυμα c του m.

Ας θεωρήσουμε το κρυπτοσύστημα του Καίσαρα. Αν αριθμήσουμε το αλφάβητο {α,β,γ,…,ω} με τους αριθμούς 0,1,2,…,23, αντίστοιχα, τότε η συνάρτηση κρυπτογράφησης είναι E(m)=(m+3) mod 24 (με κλειδί K=3).
Υποθέτουμε ότι ό χώρος μηνυμάτων’(και κρυπτογραφημένων μηνυμάτων) είναι όλες οι λέξεις με 5 χαρακτήρες, και το σύνολο των κλειδιών {0,1,…,23}.
Π.χ. E(αυριο)=E(0-20-16-8-14)=(3-23-19-11-17)=δψφμσ
Θεωρούμε την predicate f, το μήνυμα m έχει δύο ίδιους χαρακτήρες.

$$f : M = \{0,1,...,23\}^5 \to \{0,1\} \qquad f(x) = \begin{cases} 1, & \text{two characters are the same} \\ 0 & \text{else} \end{cases}$$

Τότε με πιθάνοτητα ένα μπορούμε να υπολογίσουμε την f επί οποιουδήποτε μηνύματος m, αρκεί να έχουμε την κρυπτογράφηση του c.

Πράγματι, αν στο c υπάρχουν δύο ίδιοι χαρακτήρες τότε αναγκαστικά στο m υπάρχουν δύο ίδιοι χαρακτήρες (ανεξάρτητα της επιλογής του κλειδιού.).

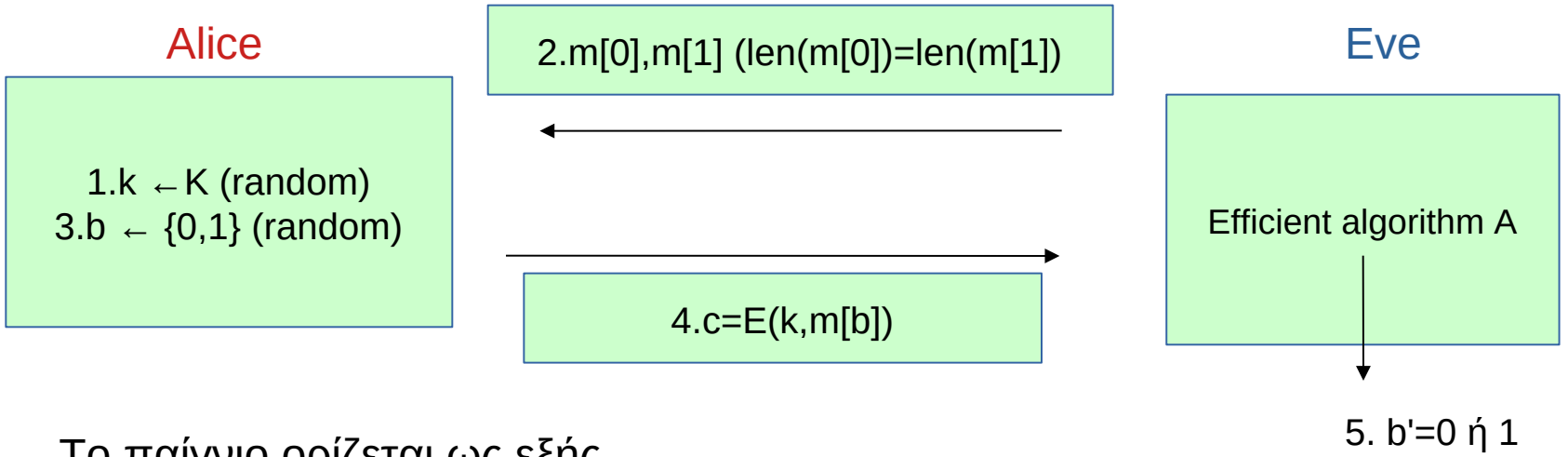


Υπάρχει και ένας δεύτερος ορισμός που βασίζεται στα παίγνια.
Αυτός ο ορισμός είναι ισοδύναμος με τον αρχικό ορισμό της σημασιολογικής ασφάλειας όπως δόθηκε προηγουμένος.

Ο ορισμός αυτός, όπως και στην περίπτωση του (δεύτερου) ορισμού της τέλειας ασφάλειας βασίζεται στην ικανότητα της Eve να μπορεί να διαχωρίσει δύο μηνύματα ίδιου μήκους.

2ος Ορισμός Σημασιολογικής Ασφάλειας (για Συμμετρικά κρυπτοσυστήματα)

Attack game between Alice and Eve



Το παίγνιο ορίζεται ως εξής

1. Η Alice διαλέγει ένα τυχαίο κλειδί.
2. Η Eve στέλνει δύο μηνύματα m[0], m[1]

=== [challenge] ===

3. Η Alice διαλέγει στην τύχη ένα bit b.
4. Η Alice κρυπτογραφεί το μήνυμα m[b].

Έστω c=E(k,m[b]) και το στέλνει στην Eve.

5. Η Eve εξάγει b'=0 ή 1.

Η Eve **κερδίζει** το παιχνίδη
αν βρει ποιο μήνυμα κρυπτογράφησε
η Alice, με πιθανότητα >1/2.

Επίσης ορίζουμε τα εξής πειράματα με την βοήθεια του προηγούμενου Παίγνιου.

Λέμε ότι εκτελέστηκε το πείραμα Exp(0) αν η Alice κρυπτογράφησε το m[0], διαφορετικά λέμε ότι εκτέλεσε το πείραμα Exp(1).

Επίσης με W[b] γράφουμε το ενδεχόμενο W[b]={A(Exp(b))=1}, όπου A ο αλγόριθμος της Eve.
Το ενδεχόμενο αυτό έχει νόημα μόνο για την Eve και όχι για την Alice, διότι για την Alice είναι το βέβαιο ενδεχόμενο, Pr(Alice,W[b]) = 1.
Η Pr(Eve,W[b]), εξαρτάται από τον αλγόριθμο A.

Τέλος, δίνουμε και τον ορισμό της συνάρτησης πλεονεκτήματος (advantage function).

Ορισμός.

$$Adv_{SS}(\mathcal{A},\mathcal{E}) = \left|P(W_0) - P(W_1)\right| = \left|P(\mathcal{A}=1|b=0) - P(\mathcal{A}=1|b=1)\right|$$

Ο **αποδοτικός** αλγόριθμος που χρησιμοποιεί η Eve.

Το κρυπτοσύστημα μας

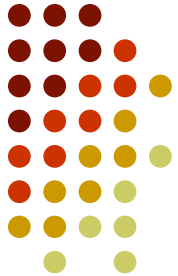
Ορισμός σημασιολογικής ασφάλειας.

Το κρυπτοσύστημα $\mathcal{E}$ ονομάζεται **σημασιολογικά ασφαλές** αν για κάθε αποδοτικό αλγόριθμο Α η συνάρτηση

$$Adv(\mathcal{A}, \mathcal{E})$$

είναι αμελητέα.

Παρατηρήσεις επί του ορισμού

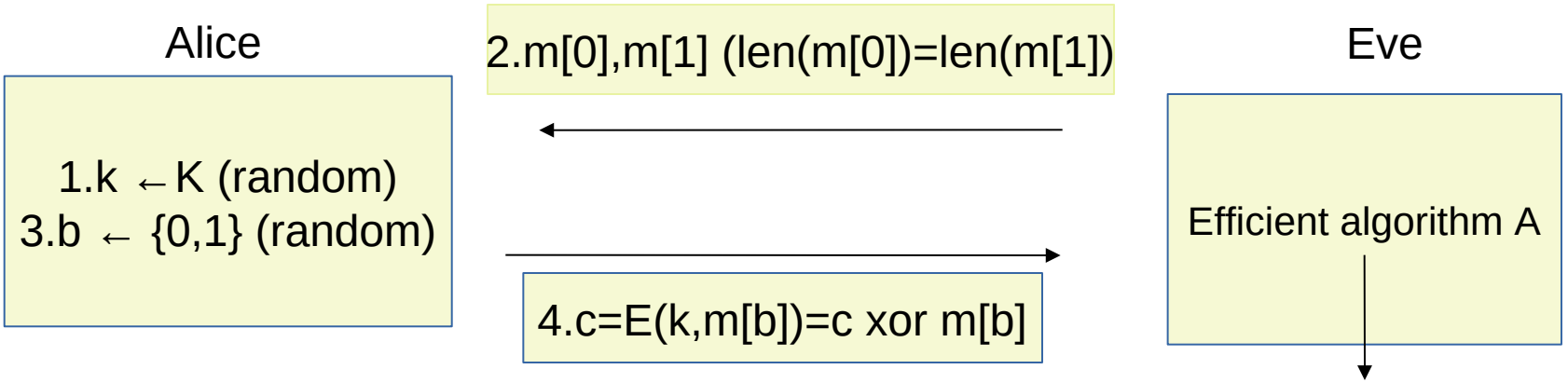


1. Όταν η συνάρτηση πλεονεκτήματος είναι κοντά στο 1, τότε το συστημα **δεν** είναι ss, διότι η Eve μπορεί να ξεχωρίσει ποιο πείραμα εκτελέστηκε.
2. Όταν είναι κοντά στο 0, το σύστημα είναι semantically secure.

Άσκηση

Αν η Eve μπορεί να εξάγει το λιγότερο σημάντικο bit του αρχικού μηνύματος, από ένα κρυπτογραφημένο μήνυμα, τότε το σύστημα δεν είναι σημασιολογικά ασφαλές. Γιατί; (να εξηγηθεί με τον ορισμό 2, διότι με τον ορισμό 1 είναι προφανές ότι δεν είναι ss).

Είναι το OTP ss;



$$Adv_{ss}(A,\mathcal{E}) = \left| Pr(A(k \oplus m[0]) = 1) - Pr(A(k \oplus m[1]) = 1) \right| = 0$$

Ίδιες κατανομές (ομοιόμορφες), διότι το κλειδί k είναι τυχαίο, οπότε από την ιδιότητα της xor, οι κατανομές είναι ομοιόμορφες.

Homework 1

1. Έστω το Ελληνικό αλφάβητο {α,β,γ,…,ω}. Δίνουμε διαδοχικά τιμές

α:0,β:1,…,ω:24. Το κρυπτοσύστημα μετατόπισης π.χ. με κλειδί k=3, ορίζεται

E(k,α)=(0+3)mod 24 = 3→δ. Δηλ. Αν το κλειδί είναι k με 0<=k<=23, τότε

E(k,X)=(αριθμητική τιμή του X + k)mod 24, ενώ η αποκρυπτογράφηση

D(k,Y)=(αριθμητική τιμή του Y - k)mod 24

Αν έχουμε να κρυπτογραφήσουμε μια λέξη εφαρμόζουμε την κρυπτογράφηση σε κάθε γράμμα ξεχωριστά.

(i) Έστω ότι έχουμε την παρακάτω κατανομή επί του χώρου μηνυμάτων

Pr[M=’α’]=0.7, Pr[M=’ω’]=0.3.

Να υπολογιστεί η πιθανότητα Pr[C=’β’].

Υπενθυμίζουμε ότι οι τ.μ. M,K (M είναι η κατανομή επι του χώρου μηνυμάτων και K η κατανομή επί του χώρου κλειδιών είναι ανεξάρτητες).

(ii) Έστω ότι έχουμε την παρακάτω κατανομή επί του χώρου μηνυμάτων

Pr[M=’ενα’]=0.3, Pr[M=’δυο’]=0.7.

Να υπολογιστεί η πιθανότητα Pr[C=’θπδ’].

Homework 2

1. Άσκηση 3.1 (από τις σημειώσεις)

2. Υπο ποιες προυποθέσεις θα μπορούσε το σύστημα του Καίσαρα να έχει τέλεια ασφάλεια ;

3. Έχουμε το εξής σύστημα. Το σύνολο μηνυμάτων και κρυπτογραφημένων μηνυμάτων είναι {0,1,2,…,100}. Το σύνολο των κλειδιών είναι οι (περιττοί) πρώτοι αριθμοί μικρότεροι του 100. Η συνάρτηση κρυπτογράφησης είναι

$$c = m^2 \mod p$$

όπου p το κλειδί (δηλ. ένας περιττός πρώτος <100).

Να εξετάσετε αν το σύστημα έχει σημασιολογική ασφάλεια.

(Π.χ. αν θέλουμε να κρυπτογραφήσουμε το μήνυμα m =100 με κλεδί 31, έχουμε c=18. Αποδεικνύεται ότι αν κάποιος έχει το c και τον πρώτο αριθμό p, μπορεί να βρεί το m (Tonelli algorithm) σε πολυωνυμικό χρόνο.).
Υπόδειξη. Σκεφτείται μια predicate που μπορείτε εύκολα να βρείτε μια ιδιότητα του m αν γνωρίζετε το c (αλλά αυτο να μπορείτε να το κάνετε για κάθε ζευγαρι (m,c)).