1η προαιρετική εργασία

Θεμελιώσεις Κρυπτογραφίας

Αναγνώστου Αντώνιος – 2268 – [anagnoad@csd.auth.gr](mailto:anagnoad@csd.auth.gr)

Λασκαρίδησ Στέφανος – 2315 – [laskstef@csd.auth.gr](mailto:Laskstef@csd.auth.gr)

2015

Περιεχόμενα

[Εισαγωγή 2](#_Toc416475622)

[Θέμα 1ο 2](#_Toc416475623)

[Υποερωτήμα i) 2](#_Toc416475624)

[Υποερώτημα ii) 2](#_Toc416475625)

[Υποερώτημα iii) 3](#_Toc416475626)

[Υποερώτημα iv) 3](#_Toc416475627)

[Θέμα 2ο 3](#_Toc416475628)

[Θέμα 3ο 3](#_Toc416475629)

[Θέμα 4ο 3](#_Toc416475630)

[Θέμα 5ο 3](#_Toc416475631)

[Θέμα 6ο 4](#_Toc416475632)

[Θέμα 7ο 4](#_Toc416475633)

[Θέμα 8ο 4](#_Toc416475634)

[Θέμα 9ο 4](#_Toc416475635)

[Υποερώτημα i) 4](#_Toc416475636)

[Υποερώτημα ii) 5](#_Toc416475637)

[Βιβλιογραφία 9](#_Toc416475638)

# Εισαγωγή

Η παρούσα εργασία αποσκοπεί στην εξοικίωση με τις βασικές έννοιες της κρυπτογραφίας, εξάσκηση με τους αλγόριθμους κρυπτογράφησης καθώς και στην εφαρμογή μεθόδων κρυπτάναλυσης για την παραβίαση κρυπτοσυστημάτων.

Για όλες τις προγραμματιστικές ασκήσεις που ακολουθούν, χρησιμοποιήθηκαν τα ακόλουθα:

* Python 3
* pycrypt library
* Sage math software
* OS: Ubuntu 14.04, 64-bit
* Github repository: https://github.com/stevelaskaridis/cryptography\_project1

# Θέμα 1ο

## Υποερωτήμα i)

**Αρχή Kerchoff:**

Σύμφωνα με την αρχή του Kerkhoff, η ασφάλεια ενός κρυπτοσυστήματος θα πρέπει να βασίζεται εξ'ολοκλήρου στη μυστικότητα του κλειδιού και στην τυχαιότητα των γεννητριών τυχαίων bitstrings. Αυτό σημαίνει πως η μυστικότητα του κώδικα και της υλοποίησης του κρυπτοσυστήματος δεν θα πρέπει να προσδίδει το στοιχείο της ασφάλειας στο σύστημά μας.

Ακόμη και αν ο επιτιθέμενος γνωρίζει τους αλγορίθμους υλοποίησης του συστήματος, δε θα πρέπει να μπορεί να "σπάσει" το κρυπτοσύστημα λόγω αυτής του της γνώσης.

Πλεονεκτήματα αυτού του κανόνα αποτελούν:

1. Ο κώδικας υλοποίησης του κρυπτοσυστήματος μπορεί να είναι open-source, με συνέπεια την παρακολούθηση και εξέτασή του από μεγαλύτερη μερίδα προγραμματιστών. ("Every bug is shallow, given enough eyes")

2. Ακόμη και αν οι γνώστες της υλοποίησης του κρυπτοσυστήματος αποτελούν τμήμα της επίθεσης προς το σύστημα, η γνώση δεν προσδίδει καμία πληροφορία σε σχέση με το κλειδί.

3. Στα πλαίσια ανοχής παραβιάσεων, αν η λειτουργία και ασφάλεια του συστήματος βασίζεται στη μυστικότητα του αλγορίοθμου υλοποίησης, αποτελεί ενδεχόμενο failure point.

## Υποερώτημα ii)

http://pileas.csd.auth.gr/file.php/141/cource-1-2-3.pdf [94]

Κρυπτοσυστήματα με τέλεια ασφάλεια:

Vigénere, OTP

<http://crypto.stackexchange.com/questions/3896/simply-put-what-does-perfect-secrecy-means>

## Υποερώτημα iii)

Όχι. Στην περίπτωση που κρυπτογραφηθούν δύο μηνύματα m1, m2 με το ίδιο κλειδί k, και τα αντίστοιχα ciphertexts είναι c1 και c2, τότε ισχύει το παρακάτω:

c1 xor c2 = (m1 xor k) xor (m2 xor k) = m1 xor m2

Αν τα μηνύματα είναι σε φυσική γλώσσα και ακολουθείται κάποια κατανομή χρήσης των γραμμάτων, τότε μπορούν να βρεθούν τα μηνύματα. Τα μηνύματα, ωστόσο, πρέπει να έχουν πλεονασμό.

## Υποερώτημα iv)

Η κατάσταση λειτουργίας σε ένα κρυπτοσύστημα τμήματος αναφέρεται στο πώς χρησιμοποιείται επαναληπτικά ο αλγόριθμος κρυπτογράφησης τμήματος για να μετασχηματίσει τμήματα τα οποία είναι μεγαλύτερα από το τμήμα (?)

**Κατάσταση λειτουργίας ECB (Electronic Codebook)**

Η απλούστερη κατάσταση λειτουργίας. Το μήνυμα διαιρείται σε blocks, καθένα από τα οποία κρυπτογραφείται αυτόνομα.

Το μειονέκτημα αυτής της μεθόδου είναι ότι επιτρέπει την ανίχνευση patterns στο κρυπτογραφημένο ciphertext, καθώς δεδομένου ότι παρόμοια blocks του μηνύματος κρυπτογραφούνται με το ίδιο κλειδί, έχουν και παρόμοιο παραγόμενο ciphertext.

# Θέμα 2ο

# Θέμα 3ο

# Θέμα 4ο

Το μήνυμα είναι το ακόλουθο:

«ΜΗΔΕΙΣ ΑΓΕΩΜΕΤΡΗΤΟΣ ΕΙΣΙΤΩ ΜΟΥ ΤΗΝ ΣΤΕΓΗΝ»

# Θέμα 5ο

Υπάρχει "bug" στη βιβλιοθήκη του zipfile όπου με διαφορετικό κωδικό του σωστού, μπορεί να γίνει extract του αρχείου με μηδενικό μέγεθος.

Στην προτεινόμενη λύση, αγνοούνται όλα τα exceptions και γίνονται οι απαραίτητοι έλεγχοι για το πότε το extraction έχει πραγματοποιηθεί επιτυχώς.

# Θέμα 6ο

# Θέμα 7ο

# Θέμα 8ο

# Θέμα 9ο

## Υποερώτημα i)

Ο αλγόριθμος Blowfish είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης τμήματος που προτάθηκε το 1993 από τον Bruce Scneier και έχει αρκετά μεγάλη διάδοση στη σημερινή εποχή. Παρέχει αποδεκτό ρυθμό κρυπτογράφησης και δεν έχει υπάρξει κάποια μέθοδος κρυπτανάλυσης που να έχει δημοσιευτεί μέχρι σήμερα. Αποτελεί εναλλακτική στο δημοφιλέστατο AES (Advanced Encryption Standard), με τον δεύτερο να έχει μεγαλύτερο μερίδιο χρήσης.

Γενικά, ο Blowfish θεωρείται πως είναι ένας αρκετά γρήγορος αλγόριθμος κρυπτογράφησης, εκτός από την περίπτωση αλλαγής κλειδιών. Κάθε νέο κλειδί χρειάζεται μία προεπεξεργασία αντίστοιχη με την κρυπτογράφηση κειμένου 4KB, το οποίο θεωρείται εξαιρετικά αργό σε σύγκριση με άλλους αλγοριίθμους. Ωστόσο, το γεγονός αυτό θα μπορούσε να λειτουργήσει και θετικά: για παράδειγμα, το OpenBSD χρησιμοποιεί έναν αλγόριθμο εμπνευσμένο από το Blowfish που αξιοποιεί αυτή την καθυστέρηση, για να αμυνθεί απέναντη σε dictionary attacks. Άλλες μετεξελίξεις του BlowFish αποτελούν οι αλγόριμοι Twofish και Threefish.

**Περιγραφή λειτουργίας:**

Ο αλγόριθμος, όπως ισχύει και στον DES και τον AES, κάνει χρήση S-boxes. Πιο συγκεκριμένα, ο Blowfish έχει block μεγέθους 64-bit και χρησιμοποιεί το σχήμα Feistel 16 φάσεων. Το μήκος του κλειδιού μεταβάλλεται από 32 μέχρι 448 bits, ενώ χρησιμοποιεί μεγάλα S-boxes που εξαρτώνται από το κλειδί.

Αναλυτικότερα, ο αλγόριθμος χρησιμοποιεί δύο subkey arrays: ένα array P 18 θέσεων, καθώς και 4 S-boxes των 256-bit. Τα S-boxes έχουν εισόδους των 8 bit ενώ το παραγόμενο αποτέλεσμα είναι 32 bit. Σε κάθε φάση χρησιμοποιείται μία μόνο θέση από το P και μετά τον τελευταίο γύρο, κάθε data block χωρίζεται στη μέση και πραγματοποιείται η πράξη XOR με μία από τις δύο εναπομείναντες θέσεις του πίνακα P.

Έχοντας πει τα παραπάνω, μπορούμε να περιγράψουμε και την συνάρτηση F του Blowfish. Η συνάρτηση αυτή χωρίζει μία είσοδο 32-bit σε 4 τμήματα των 8 bits και τοποθετεί τα bits αυτά σαν είσοδο στα S-boxes. Οι έξοδοι προστίθενται με αριθμητική modulo 2^32 και αφού πραγματοποιηθεί λογική αποκλειστική διάζευξη (XOR) παράγεται το τελικό output των 32-bit.

Η αποκρυπτογράφηση λειτουργεί με αντίστοιχο τρόπο, με την μόνη διαφορά πως οι 18 θέσεις του P (P1, P2, ..., P18) βρίσκονται σε αντίστροφη σειρά.

Όσον αφορά στην διαδικασία παραγωγής των subkeys, ο Blowfish αρχικοποιεί το P και τα S-boxes με τις δεκαεξαδικές τιμές των ψηφίων του άρρητου αριθμού π, αφού δεν υπάρχει κάποια αλληλουχία στους αριθμούς αυτούς. Έπειτα πραγματοποιείται XOR του κάθε byte του κλειδιού (επαναλμβάνοντας αυτό αν χρειαστεί), με τις θέσεις του P. Στη συνέχεια, κρυπτογραφείται ένα μηδενικό block 64 bit και το παραγόμενο κρυπτοκείμενο αντικαθιστά τα P1 και P2. Το ίδιο κρπυτοκείμενο κρυπτογραφείται ξανά, με νέα subkeys, και το νέο output αντικαθιστά τα P3 και P4. Η διαδικασία αυτή συνεχίζει, αντικαθιστώντας ολόκληρο το array P και τα S-boxes. Συνολικά δυλαδή, ο αλγόριθμος Blowfish χρειάζεται 521 περάσματα για να παράξει όλα τα subkeys.

Τρωτά σημεία:

Ο Blowfish θεωρείται ευάλωτος σε επιθέσεις όπου χρησιμοποιούνται "αδύναμα" κλειδιά. Οι χρήστες θα πρέπει να αποφεύγουν ορισμένες κλάσεις κλειδιών που είναι γνωστές για την αδυναμίες τους στη χρήση τους με τον Blowfish ή να στραφούν προς εναλλακτικές όπως ο AES, ο ChaCha (που χρησιμοποιείται από τη Google) ή ο Salsa20.

## Υποερώτημα ii)

Το bitcoin αποτελεί ένα είδος κατανεμημένου ψηφιακού συστήματος πληρωμών ανοιχτού κώδικα το οποίο εφευρέθηκε από τον/την/τους Satoshi Nakamoto. Στη βάση του, το bitcoin είναι μία δομή η οποία συνδέει λογαριασμούς με υπόλοιπο[[1]](#footnote-1) χρημάτων, ένα αντίγραφο του οποίου βρίσκεται αποθηκευμένο σε κάθε κόμβο του δικτύου.

Σημαντικό οικονομικό στοιχείο στο υπόλοιπο που συνδέεται με καθένα από τους λογαριασμούς είναι το γεγονός πως αποκτούν αξία επειδή οι ίδιοι οι χρήστες του bitcoin είναι διατεθειμένοι να ανταλλάξουν προϊόντα και υπηρεσίες έναντι bitcoin.

Η διαφορά με μία συμβατική τράπεζα είναι πως η δομή είναι απολύτως αποκεντρωμένη, και ο καθένας μέσα στο δίκτυο του bitcoin γνωρίζει για κάθε άλλη συναλλαγή, όχι μόνο για τις προσωπικές του.

Βασικά σημεία ασφαλείας που τηρούνται είναι:

* η ακεραιότητα της συναλλαγής μέσω ψηφιακών υπογραφών, referenced transactions και block chain
* η προστασία από το φαινόμενου του double spending[[2]](#footnote-2)
* η ανωνυμία των χρηστών

**Συναλλαγές**

1. Οι νέες συναλλαγές γίνονται broadcast σε όλους τους κόμβους του δικτύου
2. Κάθε κόμβος μαζεύει τις συναλλαγές σε ένα block.
3. Κάθε κόμβος δουλεύει στο να βρει τη λύση σε ένα πρόβλημα hashing[[3]](#footnote-3).
4. Όταν ο κόμβος βρει τη λύση, την κάνει broadcast σε όλους τους υπόλοιπους κόμβους.
5. Οι κόμβοι δέχονται τη συναλλαγή, μόνο αν όλες οι προηγούμενες συναλλαγές είναι έγκυρες και δεν υπάρχει double-spending.
6. Οι κόμβοι εκφράζουν την αποδοχή του block δουλεύοντας πάνω στο επόμενο block, χρησιμοποιώντας το hash του προηγούμενου block, αυτού δηλαδή που μόλις έγινε αποδεκτό.

Κάθε συναλλαγή αποτελεί μέρος του transaction chain, μίας αλυσίδας συναλλαγών που ανατρέχει μέχρι την πρώτη συναλλαγή.

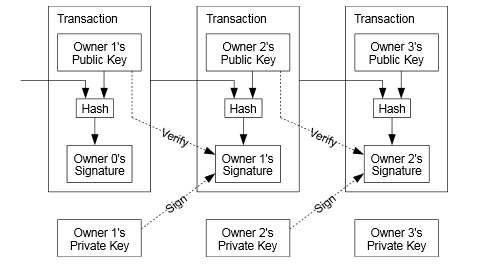
Όταν κάποιος κόμβος πραγματοποιεί μία συναλλαγή, ουσιαστικά διαδίδει (broadcasts) ένα μήνυμα με τη συναλλαγή που πραγματοποιήθηκε, υπογράφοντάς με μία μοναδική ψηφιακή υπογραφή[[4]](#footnote-4) την προηγούμενη συναλλαγή και το public key του επόμενου κατόχου του bitcoin.

Figure 1 Transaction chain

Η ψηφιακή αυτή υπογραφή είναι μοναδική για κάθε συναλλαγή, αφού εξαρτάται από το ίδιο το μήνυμα. Επιπλέον, με την ψηφιακή υπογραφή εγγυάται και η ακεραιότητα και η αυθετικότητα των δεδομένων του μηνύματος, καθώς οποιαδήποτε αλλαγή σε αυτό, θα ακύρωνε την ψηφιακή υπογραφή.

Εάν χαθεί το ιδιωτικό κλειδί ενός bitcoin wallet, χάνονται και τα bitcoins που κατέχει, όχι μόνο από τον κάτοχο, αλλά από την οικονομία του bitcoin.

**Η σειρά των συναλλαγών**

Ιδιαίτερα σημαντικό στοιχείο ασφαλείας στο bitcoin αποτελεί η σειρά με την οποία λαμβάνονται τα μηνύματα περί συναλλαγών στο δίκτυο.

Έστω ότι ο η κακόβουλη Alice στέλνει ένα ποσό σε bitcoins στον Bob. Αφού ο Bob αποστείλει το προϊόν το οποίο η Alice αγόρασε, η Alice δημιουργεί μία δεύτερη συναλλαγή, στέλνοντας τα ίδια inputs στον εαυτό της. Λόγω της δομής του δικτύου, σε κάποιους κόμβους η δεύτερη συναλλαγή θα ερχόταν πρώτη, με αποτέλεσμα να θεωρείται η συναλλαγή με τον Bob άκυρη. Ουσιαστικά θα υπήρχε διαφωνία μεταξύ των διαφορετικών κόμβων για το εάν τα bitcoins της συναλλαγής ανήκουν στο Bob ή στην Alice.

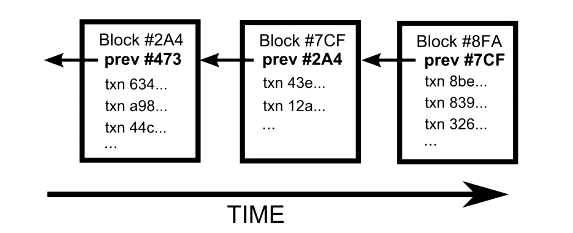
Η λύση για την κοινή γνώση περί σειράς των συναλλαγών είναι το block chaining όπου κάθε block περιέχει το hash του προηγούμενου.

Figure 2 Block Chain

Κάθε συναλλαγή η οποία θεωρείται έγκυρη, βρίσκεται μέσα στο block chain. Οι συναλλαγές οι οποίες δε βρίσκονται ακόμη εκεί, θεωρούνται μη επαληθευμένες.

Κάθε κόμβος μπορεί να ομαδοποιήσει πολλές μη επαληθευμένες συναλλαγές σε ένα block και να κάνει broadcast στο υπόλοιπο δίκτυο για το επόμενο block στο block chain.

Σε κάθε block πρέπει να περιέχεται η λύση σε ένα μαθηματικό πρόβλημα (proof of work): να βρει το input ενός hash που δημιουργήθηκε από μία cryptographic hash function (SHA256) μέσω τυχαίων guesses τα οποία συνδέονται με έναν αριθμό nonce. Σε όλο το δίκτυο του Bitcoin, παίρνει περίπου 10 λεπτά μέχρι να βρεθεί η λύση στο παραπάνω πρόβλημα. Ο πρώτος που λύσει το πρόβλημα είναι ο επόμενος του οποίου το block θα είναι η επόμενη στο transactions block chain.

Επειδή υπάρχει η περίπτωση ταυτόχρονης λύσης προβλημάτων, δημιουργούνται branches στο block chain, από τα οποία επιλέγεται το μακρύτερο ως το πιο αξιόπιστο.

Καθώς η υπολογιστική δυνατότητα του δικτύου αυξάνεται, γίνεται αναδιαμόρφωση του μαθηματικού προβλήματος ώστε τα 10 λεπτά κατά μέσο όρο για την επίλυσή του από το δίκτυο να παραμένουν σταθερά.

**Πιθανή επίθεση**

Πιθανή επίθεση double spending αποτελεί η δημιουργία ενός μακρύτερου branch στο οποίο θα χανόταν η σειρά μίας συναλλαγής. Ωστόσο, αυτό είναι ιδιαίτερα δύσκολο καθώς η κακόβουλη Alice που ηγείται της επίθεσης πρέπει να ανταγωνιστεί την υπολογιστική ισχύ όλου του υπόλοιπου δικτύου.

**Ανωνυμία χρηστών**

Η διευθυνσιοδότηση στο bitcoin network βασίζεται ουσιαστικά στα public keys του κάθε bitcoin wallet.

Αν οι συναλλαγές στο δίκτυο του bitcoin πραγματοποιηθούν από ένα δίκτυο ανωνυμίας (βλ. Tor), τότε το μόνο που συνδέει το λογαριασμό με τον κάτοχό του είναι το public key. Το σύνολο των public keys που μπορούν να χρησιμοποιηθούν στο bitcoin είναι .

Επιπλέον, για να μην μπορούν να ομαδοποιηθούν συναλλαγές bitcoin μεταξύ τους, δίνεται η δυνατότητα στο χρήστη παραγωγής νέου public key ανά συναλλαγή.

**Εξόρυξη bitcoin (Bitcoin mining)**

Ως τρόπος διανομής των bitcoins, όταν βρίσκεται η λύση σε πρόβλημα για πρόταση επόμενου block στο block chain, δίνεται κάποιο ποσό ως ανταμοιβή.

Το ποσό αυτό μειώνεται στο μισό, κάθε τέσσερα έτη. Όταν, λοιπόν δεν υπάρχουν υπόλοιπα bitcoins προς εξόρυξη, τότε η ανταμοιβή στο block θα αποτελεί κάποιο transaction fee. Συναλλαγές που δε θα έχουν transaction fee, δε θα επιλέγονται έναντι αυτών που έχουν.

Πλεονεκτήματα bitcoin

* Καμία κυβέρνηση δεν μπορεί να εκτυπώσει ή να υποτιμήσει το νόμισμα.
* Ανωνυμία συναλλασσόμενων.
* Χαμηλότερα κόστη συναλλαγών σε σχέση με τις τράπεζες.

Προβλήματα bitcoin

* Δυσκολία συναλλαγής.
* Χρήση σε παράνομες συναλλαγές με αδυναμία παρακολούθησης.
* Η εξόρυξη απαιτεί σημαντικό ποσό ενέργειας.
* Χρόνος επαλήθευσης συναλλαγής.

# Βιβλιογραφία

bitcoin.org. (n.d.). *bitcoin.org*. Retrieved from wiki.bitcoin.it: https://en.bitcoin.it/wiki/Main\_Page

Nakamoto, S. (n.d.). *Bitcoin: A peer-to-peer Electronic Cash System.* Retrieved from bitcoin.org: https://bitcoin.org/bitcoin.pdf

Wikipedia. (2015, 04 10). *Bitcoin*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Bitcoin

1. Στην ουσία το υπόλοιπο βρίσκεται με την μορφή links σε προηγούμενες συναλλαγές (transactions). Η εγκυρότητα αυτών των συναλλαγών ελέγχεται από κάθε κόμβο του δικτύου. (Transaction chain) [↑](#footnote-ref-1)
2. Αναφέρεται στην επαναχρησιμοποίηση bitcoins που έχουν ξοδευτεί. [↑](#footnote-ref-2)
3. Βιβλιογραφικά καλείται proof of work, καθώς η λύση αντανακλά τον υπολογιστικό χρόνο που έχει αφιερωθεί για την εύρεση της λύσης. [↑](#footnote-ref-3)
4. Μία ψηφιακή υπογραφή βασίζεται στις αρχές της ασύμμετρης κρυπτογραφίας, με βασικό της στοιχείο να αποτελεί πως μπορεί να επαληθευτεί η αυθεντικότητα ενός μηνύματος. [↑](#footnote-ref-4)