Εργαστηριακή Εργασία

1. Εισαγωγή

Η εργασία αυτή είναι χωρισμένη σε 3 μέρη, κάθε ένα από τα οποία ασχολείται με διαφορετικό αντικείμενο του μαθήματος, το οποίο έχουμε καλύψει στα πλαίσια των διαλέξεων.

Τις απαντήσεις σας στις ερωτήσεις θα τις καταγράψετε σε αρχείο που θα ονομάσετε χρησιμοποιώντας το επώνυμο και τον αριθμό μητρώου σας ως εξής: SecurityProject2020_PAPADOPOULOS_6074.docx). Όταν ολοκληρώσετε την εργασία, ζητείται να ανεβάσετε τις απαντήσεις σας στην ιστοσελίδα του μαθήματος. Μπορείτε να ανεβάσετε πάνω από μία φορά τις απαντήσεις σας αντικαθιστώντας το παλαιό σας αρχείο. Όταν κάνετε τελική υποβολή εργασίας, κλειδώνεται το κείμενό σας και δεν μπορείτε να κάνετε τροποποίηση. ***Παρακαλείστε να ανεβάσετε το αρχείο απαντήσεών σας σε .pdf format.***

Στην αρχή της εργασίας σας, παραθέστε το ακόλουθο πινακάκι με τα στοιχεία σας:

Ονοματεπώνυμο:
Αριθμός Μητρώου:
Εξάμηνο:
Πρώτο πτυχίο:

Επισημαίνεται ότι η εργασία αυτή είναι ατομική.

Η καταληκτική ημερομηνία παράδοσης της εργασίας ορίζεται στις **25/01/2020**.

2. Κλασσικοί Αλγόριθμοι Κρυπτογράφησης

Στο κομμάτι αυτό της εργασίας θα μελετηθούν αντιπροσωπευτικοί κλασσικοί αλγόριθμοι κρυπτογράφησης. Θα χρησιμοποιηθεί το εργαλείο Cryptool 2.1, το οποίο αποτελεί πλατφόρμα για κρυπτογράφηση και κρυπτανάλυση. Το CrypTool διαθέτει εύχρηστα built-in tutorials και documentation και μπορείτε να το κατεβάσετε από το σύνδεσμο https://www.cryptool.org/en/ct2-downloads.

Όπου ζητείται screenshot από το CrypTool, θα πρέπει να σώζετε το project σας με όνομα αρχείου το ονοματεπώνυμό σας με λατινικούς χαρακτήρες, underscore αύξοντα αριθμό της ερώτησης (π.χ., PAPADOPOULOSNIKOS_1.cwm) και να κάνετε print screen + paste στο αρχείο που θα παραδώσετε, ώστε να φαίνεται και το όνομα του project.

Σχετική ύλη: Αλγόριθμοι Αντικατάστασης (substitution): Monoalphabetic Cipher (Caesar Cipher), multiple-letter encryption ciphers (Playfair Cipher, Hill Cipher, Vigenere Cipher, Vernam Cipher), Αλγόριθμοι Αντιμετάθεσης (transposition or permutation): Rail Fence Cipher, Columnar Transposition Ciphers. Κρυπτανάλυση: Κρυπταναλυτική επίθεση,

Σας ζητείται να κάνετε σύγκριση αλγορίθμων αντικατάστασης, μονοαλφαβητικών και πολυαλφαβητικών ως προς την ασφάλεια και την ανθεκτικότητα σε τεχνικές κρυπτανάλυσης συχνότητας.

Ζητούνται τα ακόλουθα:

1. Ξεκινώντας από κείμενο δική σας επιλογής μεγέθους της τάξεως των 2000 λέξεων και κάνοντας χρήση του εργαλείου Cryptool πραγματοποιήστε κρυπτογράφηση βάσει αλγορίθμων αντικατάστασης Ceasar, Playfair, Hill, Vigenere και Vernam. Για να το επιτύχετε, θα κάνετε χρήση των έτοιμων αντιστοίχων αλγορίθμων (blocks) του Cryptool καθώς και Text Input για να εισάγετε το απλό κείμενο και Text Output για να λάβετε το κρυπτοκείμενο.

2. Πραγματοποιήστε ανάλυση συχνότητας με τη βοήθεια του Cryptool και του Frequency Test block που διαθέτει και σχολιάστε με βάση τις συχνότητες την ανθεκτικότητα κάθε αλγορίθμου που δοκιμάσατε. Εντοπίστε τα αδύναμα σημεία του καθενός και τις παραμέτρους από τις οποίες εξαρτάται η απόδοσή τους.

3. Κρυπτογραφήστε το ίδιο κείμενο κάνοντας χρήση του αλγόριθμου Transposition, πραγματοποιήστε ανάλυση συχνότητας και καταγράψτε τις παρατηρήσεις σας.

Υπενθυμίζεται ότι θα πρέπει στην εργασία που θα υποβάλλετε να παραθέσετε screenshots από όλα τα projects που χρησιμοποιήσατε.

3. Σύγχρονοι Αλγόριθμοι Κρυπτογράφησης

Στο κομμάτι αυτό της εργασίας θα μελετηθούν αντιπροσωπευτικοί σύγχρονοι αλγόριθμοι κρυπτογράφησης. Θα χρησιμοποιηθεί το εργαλείο Cryptool 2.1, το οποίο αποτελεί πλατφόρμα για κρυπτογράφηση και κρυπτανάλυση. Το CrypTool διαθέτει εύχρηστα built-in tutorials και documentation.

Όπως και πριν, όπου ζητείται screenshot από το CrypTool, θα πρέπει να σώζετε το project σας με όνομα αρχείου το ονοματεπώνυμό σας με λατινικούς χαρακτήρες, underscore αύξοντα αριθμό της ερώτησης (π.χ., PAPADOPOULOSNIKOS_1.cwm) και να κάνετε print screen + paste στο αρχείο που θα παραδώσετε, ώστε να φαίνεται και το όνομα του project.

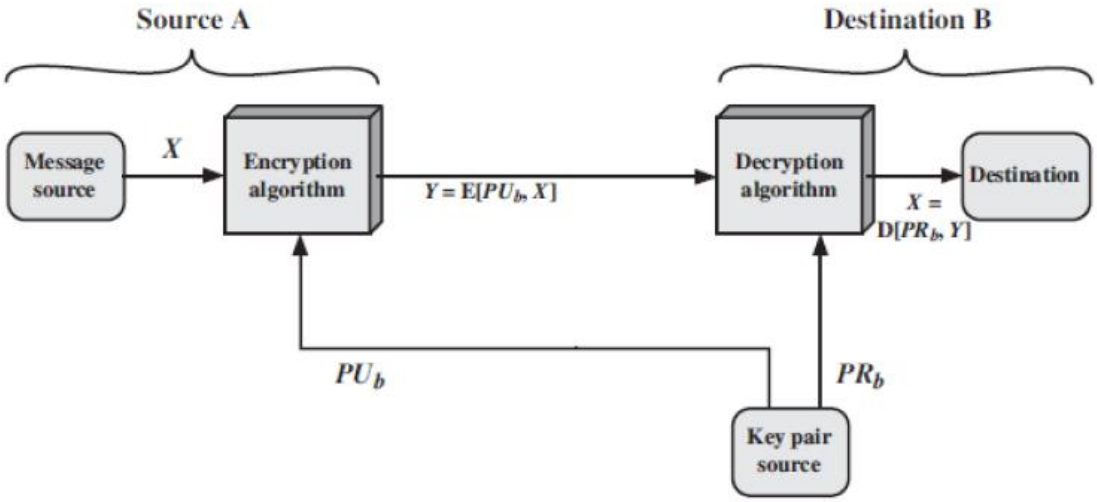
Σχετική ύλη: Συμμετρικοί αλγόριθμοι: XOR, DES, TripleDES, AES. Κρυπτογράφηση δημοσίου Κλειδιού: RSA.

Ζητούνται τα ακόλουθα:

1. Ξεκινώντας από κείμενο δική σας επιλογής (τουλάχιστον 10000 Bytes) και κάνοντας χρήση του Cryptool πραγματοποιήστε κρυπτογράφηση κάνοντας χρήση συμμετρικών αλγορίθμων κρυπτογράφησης XOR, DES, TripleDES, AES χρησιμοποιώντας κλειδί κατάλληλου μήκους δικής σας επιλογής. Στη συνέχεια πραγματοποιήστε ανάλυση συχνότητας και σχολιάστε με βάση τις συχνότητες την ανθεκτικότητα των αλγορίθμων, εντοπίζοντας τα πλεονεκτήματα και τα μειονεκτήματά τους.

2. Με χρήση του Cryptool και του RSA αλγορίθμου που διαθέτει, παράγετε ζεύγος κλειδιών για τους χρήστες a και b κάνοντας χρήση του RSA Key Generator block.

3. Υλοποιήστε με το CrypTool διάταξη για την προστασία της εμπιστευτικότητας (confidentiality) μηνύματος της επιλογής σας σύμφωνα με το ακόλουθο σχήμα:

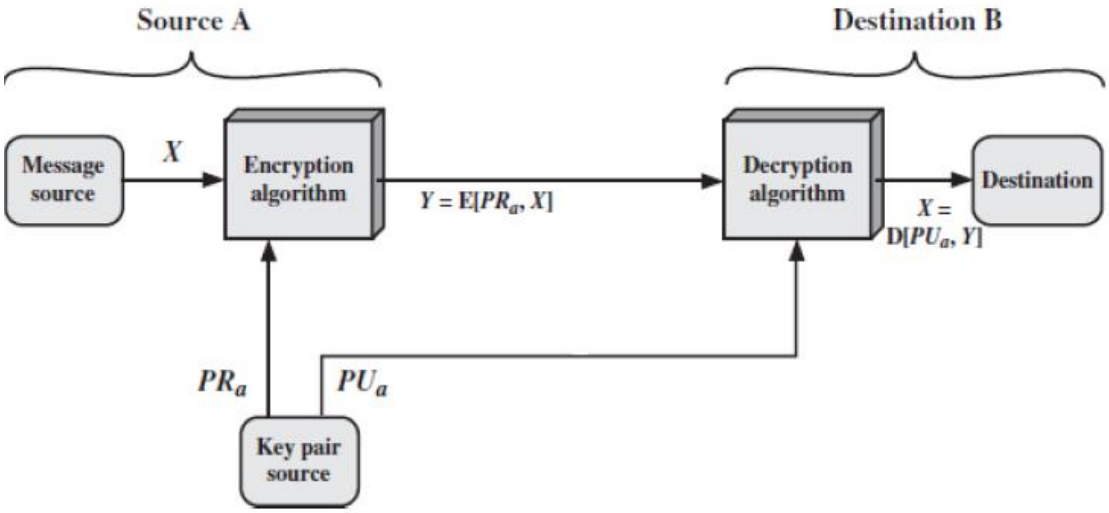


Ο χρήστης a κρυπτογραφεί το μήνυμα X με το public key του παραλήπτη b. Στη συνέχεια ο παραλήπτης χρησιμοποιεί το private key του για την αποκρυπτογράφηση του μηνύματος.

Y = E(PUb, X), X = D(PRb, Y)

4. Υλοποιήστε με το CrypTool διάταξη για την πιστοποίηση της ταυτότητας (authentication) κάποιας οντότητας (π.χ., χρήστης) αλλά και για την διασφάλιση ότι το μήνυμα δεν έχει υποστεί αλλαγές (integrity), όπου ο χρήστης a κρυπτογραφεί το μήνυμα X με το private key του. Στη συνέχεια ο παραλήπτης χρησιμοποιεί το public Key του a για την αποκρυπτογράφηση του. Επιτυχημένη αποκρυπτογράφηση πιστοποιεί ότι όντως έχει κρυπτογραφηθεί με το private key που γνωρίζει μόνο ο χρήστης a.

Y = E(PRa, X), X = D(PUa, Y)



Υπενθυμίζεται ότι θα πρέπει στην εργασία που θα υποβάλλετε να παραθέσετε screenshots από όλα τα projects που χρησιμοποιήσατε.

4. Ανίχνευση εισβολής

Στο κομμάτι αυτό της εργασίας θα μελετηθεί η ανίχνευση εισβολής με χρήση του εργαλείου Snort (https://www.snort.org/downloads) και του εργαλείου Wireshark (https://www.wireshark.org/download.html), τα οποία θα πρέπει να κατεβάσετε και να εγκαταστήσετε.

Ανοίξτε ένα παράθυρο εντολών και μεταβείτε στον κατάλογο **C:\snort\bin.**
Πληκτρολογήστε "**snort –h**" και πιέστε **Enter** για να δείτε το snort help. Εξετάστε τη χρήση των ακόλουθων εντολών:

snort -W

snort -i <if>

snort -v

snort -d

snort -e

snort -b

snort -l <ld>

snort -K <mode>

snort -c <rules>

snort -r <tf>

snort -x

snort –X

Ζητούνται τα ακόλουθα:

1. Εντοπίστε τη διεπαφή του υπολογιστή σας μέσω της οποίας έχετε δικτυακή κίνηση. Στη συνέχεια ξεκινήστε με την εντολή snort –v –i?, όπου ? ο αριθμός της προηγούμενης διεπαφής, καταγραφή στη διεπαφή αυτή. Σε νέο παράθυρο εντολών εκτελέστε εντολή ping προς προορισμό της επιλογής σας. Στο αρχείο απαντήσεων αντιγράψτε το σχετικό screenshot της καταγραφής του snort.

2. **Snort Packet Logger Mode**: Χρησιμοποιείστε το Snort για την καταγραφή πακέτων σε αρχείο ορίζοντας συγκεκριμένο φάκελο καταγραφής χρησιμοποιώντας την παράμετρο –l.

   Η εντολή αυτή καταγράφει όλα τα ανιχνευόμενα πακέτα σε log file.

Χρησιμοποιήστε έναν internet browser και επισκεφτείτε μία ιστοσελίδα της επιλογής σας. Με το wireshark μπορείτε να διαβάσετε το log αρχείο που δημιουργήθηκε. Στο αρχείο απαντήσεων αντιγράψτε σχετικό screenshot από το wireshark. Το log αρχείο μπορείτε επίσης να διαβάσετε με το Snort χρησιμοποιώντας την επιλογή **-r**, η οποία ξεκινά λειτουργία αναπαραγωγής των καταγεγραμμένων πακέτων (playback mode). Στο αρχείο απαντήσεων αντιγράψτε σχετικό screenshot.

3. Θα κάνετε χρήση της δυνατότητας του snort να χρησιμοποιεί κανόνες κατά την καταγραφή. Οι κανόνες είναι αυτής της μορφής:

   action protocol address port direction address port (rule option)

   Το πεδίο action προσδιορίζει τη βασική ενέργεια που πρέπει να εκτελεστεί, εάν οι τιμές των υπολοίπων πεδίων συμφωνούν με τα αντίστοιχα πεδία πακέτου που ανιχνεύτηκε. Η βασική τιμή του πεδίου αυτού, όταν το Snort λειτουργεί ως Packet Logger είναι “log”, η οποία οδηγεί σε καταγραφή πακέτων σε log file, η τυπική θέση του οποίου είναι στο φάκελο C:\snort\log. Το πεδίο protocol μπορεί να είναι "TCP", "UDP" ή "ICMP". Η τιμή "Any" δεν υποστηρίζεται. Το πεδίο address προσδιορίζεται με τυπική CIDR σημειογραφία διευθύνσεων. Το πεδίο port αποδίδεται ως ένας φυσικός αριθμός (που αντιστοιχεί σε θύρα) ή ως διάστημα αριθμών, ενώ μπορεί να χρησιμοποιηθεί και ο τελεστής "!" για να εξαιρέσει θύρες. Το πεδίο direction είναι ίσο με "->" ή "<-", για μονόδρομη κίνηση, ή "<>" για αμφίδρομη κίνηση μεταξύ δύο διευθύνσεων. Το πεδίο rule option προσδιορίζει επιπλέον ενέργειες/συνθήκες που πρέπει να εκτελεστούν/ελεγχθούν, σε περίπτωση που οι καθορισμένες διευθύνσεις και τα πρωτόκολλα ανιχνευτούν. Σημειώνεται ότι στις παρενθέσεις μπορεί να ορίζονται περισσότερες από μία παράμετροι. Η έκφραση κάθε μιας πρέπει να καταλήγει σε “;”, ακόμη κι αν είναι η μοναδική παράμετρος του κανόνα. Κάθε κανόνας πρέπει να έχει μοναδική ταυτότητα, η οποία ορίζεται από την παράμετρο “sid”. Άλλες χρήσιμες παράμετροι είναι: “msg”, “itype”, “content”, “flags”, “length”, “dsize”, “ttl”, κ.α. ναλυτικός κατάλογος των Rule Options είναι διαθέσιμος στο εγχειρίδιο χρήσης του Snort (http://manual.snort.org/snort_manual.html).

   Συντάξτε κανόνα που θα αφορά κίνηση προς την πόρτα 80 (http) ή 443 (https) της ιστοσελίδας που επιλέξατε προηγούμενα και σώστε τον σε αρχείο txt κάτω από το φάκελο c:\snort\rules. Στη συνέχεια με την παράμετρο –r διαβάστε το αρχείο καταγραφής του προηγούμενου ερωτήματος κάνοντας χρήση του κανόνα που φτιάξατε με χρήση της παραμέτρου –c. Στο αρχείο απαντήσεων αντιγράψτε τον κανόνα και το αποτέλεσμα του snort.

4. Συντάξτε κανόνες που θα απομονώνουν κίνηση http, SMTP, ftp και telnet. Στο αρχείο απαντήσεων αντιγράψτε τους κανόνες.

5. **Snort Network Intrusion Detection System Mode:** Σε αυτό μέρος της άσκησης θα μελετήσουμε το Network Intrusion Detection System – NIDS Mode του Snort. Όταν το Snort λειτουργεί σε NIDS mode, υπάρχουν διάφορες ενέργειες (actions), που χρησιμοποιούνται στους κανόνες, όπως οι ακόλουθοι:

- alert: δημιουργεί ειδοποίηση χρησιμοποιώντας την επιλεγμένη μέθοδο ειδοποίησης, και στη συνέχεια καταγράφει το πακέτο σε αρχείο (Προσοχή: όλες οι ειδοποιήσεις αποθηκεύονται σε ένα κοινό αρχείο alert, η συνήθης θέση του οποίου είναι στο φάκελο C:\Snort\log.)
- log: καταγράφει το πακέτο σε αρχείο (Προσοχή: κάθε διεύθυνση IP αποκτά το δικό της φάκελο με τα δικά της αρχεία καταγραφής για μεταγενέστερη ανάλυση, η συνήθης θέση των οποίων είναι στο φάκελο C:\Snort\log.)
- pass: αγνοεί το πακέτο σιωπηρά και δεν το προωθεί στον προορισμό του
- activate: δημιουργεί ειδοποίηση και, στη συνέχεια, ενεργοποιεί ένα άλλο δυναμικό κανόνα
- dynamic: παραμένει αδρανής έως ότου ενεργοποιηθεί από έναν κανόνα activate, οπότε λειτουργεί ως κανόνας log
- drop: μπλοκάρει το πακέτο και το καταγράφει σε αρχείο
- reject: μπλοκάρει το πακέτο, το καταγράφει σε αρχείο και στη συνέχεια αποστέλλει μήνυμα "TCP reset" (αν το πρωτόκολλο είναι TCP) ή "ICMP port unreachable" (εάν το πρωτόκολλο είναι UDP).
- sdrop: μπλοκάρει το πακέτο, αλλά δεν το καταγράφει σε αρχείο

Όταν το Snort λειτουργεί σε NIDS mode, δεν καταγράφει κανονικά όλα τα πακέτα που έχουν συλληφθεί, όπως γίνεται όταν λειτουργεί σε network sniffer mode. Αντ' αυτού, εφαρμόζει τους κανόνες που έχει σε όλα τα πακέτα που συλλαμβάνει. Εάν ένα πακέτο ταιριάζει με ένα κανόνα, μόνον τότε είναι καταγράφεται σε αρχείο ή παράγεται ειδοποίηση. Εάν ένα πακέτο δεν ταιριάζει με κανένα κανόνα, το πακέτο απορρίπτεται σιωπηλά και δεν καταχωρείται στο αρχείο καταγραφής. Όταν το Snort χρησιμοποιείται σε NIDS mode, συνήθως παραμετροποιείται από το διαχειριστή από ένα αρχείο ρυθμίσεων (configuration file), το οποίο ενεργοποιείται με τη γραμμή εντολών. Αυτό το αρχείο διαμόρφωσης περιέχει κανόνες Snort ή αναφορά σε άλλα αρχεία που περιέχουν κανόνες Snort. Εκτός από τους κανόνες, το αρχείο ρυθμίσεων περιέχει επίσης πληροφορίες σχετικά με plug-ins εισόδου και εξόδου. Το τυπικό όνομα του αρχείου ρυθμίσεων του Snort είναι snort.conf.

Ζητείται να αναζητήσετε στο διαδίκτυο malware trace files (pcap αρχεία), τα οποία θα διαβάσετε με το Wireshark, να τα μελετήσετε και να εντοπίσετε τα πακέτα που οφείλονται στο συγκεκριμένο malware. Γράψετε τον τρόπο λειτουργίας του malware και στη συνέχεια συντάξτε κανόνες στο snort που θα στέλνουν και θα καταγράφουν alert μόλις ανιχνευτεί κάποιο από τα ύποπτα πακέτα, με μήνυμα: "Malware detected by <το ονοματεπώνυμό σας με λατινικούς χαρακτήρες>!!!" και να αναπαράγετε τα δεδομένα trace files με το Snort, υπό τους κανόνες που συντάξατε για ανίχνευση της εισβολής αυτής. Παραδείγματα δικτυακών τόπων διάθεσης pcap αρχείων είναι τα ακόλουθα (στα οποία μπορείτε να καταφύγετε εάν δεν εντοπίσετε εναλλακτικές):

- https://www.malware-traffic-analysis.net/
- https://www.pcapanalysis.com/download-malware-samples/