Assignment 1

1)

2) a.

3) a.

Ciphertext-only attack - is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts.

Known-plaintext attack - is an attack model for cryptanalysis where the attacker has access to both the plaintext, and its encrypted version (ciphertext).

Chosen-plaintext attack - is an attack model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme.

Chosen-ciphertext attack - is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts. From these pieces of information, the adversary can attempt to recover the hidden secret key used for decryption.

b.

As we saw the example in PS-4 on attacking RSA with 2 messages and their cyphers:

RSA has Multiplicative attribute, that means RSA {M1 \* M2}n,e = RSA {M1}n,e \* RSA {M2}n,e

And, RSA-1{C1 \* C2}n,d = , RSA-1{C1}n,d \* , RSA-1{C2}n,d.

With this in mind, we can increase our pairs by doing the following:

We choose our C2 or C1 (works both ways), and for every C and suffices this equation

C2 = C/C1mod(n), we can add him and his decrypted message to our pairs. We know C1 and C2 decryptions, so we know M = M1 \* M2 mod(n).

The attacker cannot exploit this attack if both C1 and C2 are bigger than N thus we will not be able to suffice our equation.

//TODO

4) a.

הבעיתיות שנוצרה בהגדרת הפרוטוקול היא שהוא פגיעה למתקפות man in the middle, כמו שהוסבר בכיתה, התוקף יקבל את ההודעות עם המפתחות וישלח מפתח חדש משלו לכל צד וככה הוא ינתר וישבש את התקשורת ביניהם.

b.

כדי להתגבר על הבעייתיות ניתן להוסיף חתימה דיגיטלית למפתחות ,וכך למנוע את המתקפות של MITM. בנוסף למפתח הפרטי המוצפן שאליס או בוב ירצו לשלוח, יהיה עוד שלב של חתימה דיגיטלית להודעה בעזרת המפתח הפרטי של השולח, והמקבל יוודא את ההודעה בעזרת המפתח הפומבי של השולח. כך נוכל למנוע התערבות של צד שלישי מכיוון שאם ישנה את תוכן ההודעה בין אם ישאיר את החתימה הקודמת או שיעשה אחת משלו, המקבל יצליח לזהות שהייתה בעיה מכיוון שלתוקף אין את המפתח הפרטי של השולח, וניתן לוודא הודעה שהוצפנה עם מפתח פרטי רק בעזרת המפתח הפומבי של השולח.

5)

הנתון הבא מתייחס לכל הסעיפים: מכיוון שיש גישה לתיקיית ה-tmp נוכל לתקוף שם בעזרת שיטת meet-in-the-middle כמו שלמדנו ב-2DES.

a.

נשלח הודעה M ונגנוב את ההצפנה שלה C1, נעבור על כל הקומבינציות האפשריות כמו שלמדנו בכיתה ע"י הצפנה של M כמו שרשום בתרגיל ונתרגם את C1 גם עם כל הקומבינציות וע"י lookup נוכל למצוא את הקומבינציות האפשריות ל-K1 ו-K2, נריץ הצפנה עם הקומבינציות האפשריות ונמצא את המפתחות האמיתיים. לגבי K3,K4,K5 נפצח אותם בעזרת 3 לולאות brute-force.

זמן ריצה: (562)O , להצפנה + פענוח + חיפוש. זכרון: (562)O , טבלאת ה-lookup.

b.

כמו שרשום בתחילת הסעיף הקודם נתקוף את tmp בעזרת MITM ונקבל את מפתחות K1,K2 , לכן נשאר לנו רק לפצח את K3, ועליו פשוט נעבור בעזרת כל הקובינציות לכן:

זמן ריצה: (572)O , להצפנה + פענוח + חיפוש + מציאת מפתח אחרון. זכרון: (562)O , טבלאת ה-lookup.

c.

ניתן לראות שהמפתח הראשון והשני זהים לכן C1 = M, לכן אין צורך אפילו לפצח את K1, נשאר לפצח את 3 המפתחות הנותרים, ואפשר לראות שזוהי הצפנת 3DES, ולכן הזמן ריצה: (1682)O , זכרון: (1)O .