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.

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 את התקשורת ביניהם.

b.