1- Prove that Elgamal's signature scheme works (the verification process).

2- Prove that RSA also works when gcd(M,n)≠ 1.

Hint: you may use Fermat's little theorem instead of Euler's. Alternatively, you can use Chinese Remainder Theorem.

3- A bank uses a biometric system to authenticate employees entering the safe where the money is stored overnight. To get in the room, one has to type in the username and put his/her finger on the sensor. The fingerprint is then digitalized and sent to the authentication server, which accepts or rejects access to the room. The authentication server relates the username with the digital version of the fingerprint. Statistical analysis shows that the authentication server has a false-reject rate of 10% and a false-accept rate of 0.5%. The user is allowed to try five attempts, after which security guards are called and the user is locked up.
a) Explain what false-accepts and false-rejects are.
b) What is the probability that a valid user is locked up by mistake?
c) what is the probability that an invalid user is granted access? Are the above-mentioned rates suitable for this kind of application?

4. Consider the following protocol that lets A and B agree on a new session key like K'_{AB}. Assume that these users had shared K_{AB} before.

1. $A \rightarrow B: A, N_A$
2. $B \rightarrow A: \mathrm{E}(K_{AB}, [N_A, K'_{AB}])$
3. $A \rightarrow B: \mathrm{E}(K'_{AB}, N_A)$

a) Why do A and B think they have agreed on K'_{AB} with the other person at the end of the protocol?

Write your reason in the standard form:

- A thinks he has shared K'_{AB} with B because ….
- B thinks he has shared K'_{AB} with A because ….
- A thinks K'_{AB} is fresh because ….
- B thinks K'_{AB} is fresh because ….

b) now imagine the channel has been intercepted and Eve (C) is in the middle. A wants to run the protocol with B, but C is in the middle and runs the protocol with A on behalf of B. while A thinks he has made a new key with B, he was actually communicating with C. If both parties can ask the other one to refresh the session key at any time, show how one can attack this protocol. This shows that our judgment in part a was not flawless.

c) propose a solution to fix this vulnerability.

5- Consider the following protocol. It's similar to Needham-Schroeder protocol we saw in the class:

1. A→KDC: $\mathrm{ID_A} \parallel \mathrm{ID_B} \parallel \mathrm{N_1}$
2. KDC→ A: $\mathrm{E}(K_a, [K_S \parallel ID_B \parallel N_1 \parallel \mathrm{E}(K_b, [K_S \parallel ID_A]))$
3. A→ B: $\mathrm{E}(K_b, [K_S \parallel ID_A])$
4. B→A: $\mathrm{E}(K_S, N_2)$
5. A→B: $\mathrm{E}(K_S, \mathrm{f}(N_2))$

a) Explain the protocol steps.

b) Can you think of a possible attack on this protocol? Explain how it can be done.

c) Mention a possible technique to get around the attack—not a detailed mechanism,

just the basics of the idea.

6- Consider the following protocol. The goal of the protocol is to distribute a new session key between A and B using a pre-shared key.

$$A \rightarrow B:\ A, \{N_a\}_{K_{ab}}$$
$$B \rightarrow A:\ \{N_a + 1, N_b\}_{K_{ab}}$$
$$A \rightarrow B:\ \{N_b + 1\}_{K_{ab}}$$
$$B \rightarrow A:\ \{K'_{ab}, N'_b\}_{K_{ab}}$$

We make the following assumptions in BAN logic language:

$$A \text{ believes } A \overset{K_{ab}}{\longleftrightarrow} B,\ B \text{ believes } A \overset{K_{ab}}{\longleftrightarrow} B$$
$$B \text{ believes } A \overset{K'_{ab}}{\longleftrightarrow} B$$
$$A \text{ believes } (B \text{ controls } A \overset{K'_{ab}}{\longleftrightarrow} B),$$
$$A \text{ believes } fresh(N_a),\ B \text{ believes } fresh(N_b),$$
$$B \text{ believes } fresh(N'_b)$$

The goal is to prove:

$$B \text{ believes } A \overset{K'_{ab}}{\longleftrightarrow} B,\ A \text{ believes } A \overset{K'_{ab}}{\longleftrightarrow} B$$

Idealize the protocol and if possible, prove the goals using BAN logic rules. If it's not possible, describe the potential problem and design an attack according to your findings.