Question 1. (40 pts.) Answer briefly each of the following questions:

a. Why may a slow key schedule be desirable for a cipher? (e.g. Blowfish) Explain briefly.

b. In which of the ECB, CBC, OFB, CFB, and CTR modes of operation, is encryption parallelizable?

c. Is a fixed or a random IV preferable in a CBC-MAC computation? Why?

d. What is the role of the “compression function” in the structure of a hash function? (I.e., describe the operation of a hash function according to the compression function.)

e. As MACs can be produced from hash functions, consider producing a hash function from CBC-MAC, where the CBC checksum of a message is computed using a fixed key and IV. Would this hash function be secure? Why/why not?

f. Is a fixed or random padding used in the PKCS for RSA signature? Why?

g. Can the ElGamal encryption system be used as a signature algorithm in a straightforward manner—using the private key operation for signing and the public key operation for verification? Why/why not?

h. A dishonest dealer might distribute “bad” shares for a Shamir threshold scheme, i.e., shares for which different $t$-subsets determine different keys. Given all $n$ shares, we could test the consistency of the shares by computing the key for every one of the $\binom{n}{t}$ $t$-subsets of participants, and verifying that the same key is computed in each case. Describe a more efficient method for testing the consistency of the shares.
Question 2. (20 pts.) Consider the following mode of encryption with three keys $k, k_1, k_2$, where $k$ is of the length of the block size and $k_1$ and $k_2$ are of the length of the key size (denoted by $\ell$) of the block cipher $E$. (E.g., for DES, $k$ would be 64 bits, and $k_1$ and $k_2$ would be 56 bits each.)

![Encryption Diagram]

a. Describe the decryption operation for this mode of encryption.

b. Describe a known-plaintext attack with a relatively small number of input blocks (e.g., with 20 or 30 blocks) where the attacker can discover the full key $(k; k_1; k_2)$ with approximately $2 \cdot 2^\ell$ runs of the encryption/decryption algorithm. (You can assume as much memory as you need for the attack.)

c. Comment on the security of this mode of encryption as a potential way of strengthening DES with an increased key size.

Question 3. (20 pts.) Consider a variant of the ElGamal signature scheme where $p; g; \alpha; \beta; k; r$ are as in the original scheme as described in class and

$$s = (r\alpha + k)m^{-1} \mod (p - 1),$$

where you can assume that $m$ is always relatively prime to $p - 1$.

a) What would the signature verification formula be for the modified scheme? (Put your answer in a frame.)

b) Show that this ElGamal variant is insecure. (Hint: Show that attacker Eve who has observed the signature of a message $m$ can obtain the signature of any message she likes.)

Question 4. (20 pts.) Alice computes her RSA signatures in an optimized way by first computing $y_p = x^d \mod p$, $y_q = x^d \mod q$, and then obtaining $y = x^d \mod n$ by the Chinese Remainder Theorem. During the signature of a message, while $y_p$ was being computed, a glitch at Alice’s computer caused it to produce a wrong value $\tilde{y}_p$ different from $y_p$. Then the computation of $y_q$ proceeded without any errors. At the end, a wrong signature $\tilde{y}$ was obtained from $\tilde{y}_p$ and $y_q$.

a) Show that any person who observes the message $x$ with the wrong signature $\tilde{y}$ can factor Alice’s modulus $n$. (Hint: Use the fact that $\tilde{y}^e \equiv x \mod q$.)

b) Suggest some method by which Alice can defend against this danger.

*Good luck!*