Solutions for Assignment 10

1. Let $pk = (\mathbb{G}, q, g, h)$ be the public-key and $sk = x = \log_g h$ be the secret-key for El Gamal encryption scheme. Let a PPT adversary obtains a ciphertext $c = (c_1, c_2)$ of some unknown plaintext m, encrypted as per the El Gamal encryption scheme, using the above public key. The adversary picks a uniformly random r' from $\mathbb{Z}_q$, where $|\mathbb{G}| = q$ and computes $c' = (c_1 \cdot g^{r'}, c_2 \cdot m' \cdot h^{r'})$.

   a. c' on decryption will output $(m')^m$

   b. c' on decryption will output $m + m'$

   c. c' on decryption will output $(m)^{m'}$

   d. c' on decryption will output $m \cdot m'$

   As per the semantics of El Gamal encryption scheme, we have that $c_1 = g^r$ for some $r \in \mathbb{Z}_q$ and $c_2 = h^r \cdot m$. It then follows that $c_1 \cdot g^{r'}$ will be $g^{r+r'}$ and $c_2 \cdot m' \cdot h^{r'}$ will be $h^{r+r'} \cdot (m \cdot m')$. Hence c' will be a valid ciphertext for the plaintext $m \cdot m'$, as per the randomness $r + r'$ and hence c' upon decryption will output $m \cdot m'$. So the answer is **d**.

2. Suppose in RSA cryptosystem, we have an e, which has at least one 0 in its binary representation. Now let e' be another RSA public key, obtained by flipping one of the 0 bit in the binary representation of e to 1. Then

   a. e and e' are not co-prime

   b. e' will be even

   c. e and e' are co-prime

   d. Can't determine the relation between e and e'

   As both e and e' are RSA keys, they have to be odd, as both of them are co-prime to $\phi(N)$, which is an even quantity. Suppose e' is obtained by flipping the i^{th} bit of e from 0 to 1. Hence $e' = e + 2^i$. Since e is odd, it cannot have an even divisor and hence all the divisors of e are odd. But no divisor of e (which is an odd quantity) can divide 2^i and hence it cannot divide $e + 2^i$, which is the same as e'. Hence we get that e and e' are co-prime. So the answer is **c**.

3. Choose the correct option(s):

   a. Key generation in case of El Gamal requires less number of values to be computed as compared to RSA

   b. El Gamal crypto system when instantiated with elliptic curve provides higher security with the smaller key lengths compared to RSA

   c. Sharing El Gamal public parameters with more than one receiver is insecure

   d. El Gamal encryption scheme is only COA secure and not CPA secure

   The first statement is correct, as the number of values which need to be generated in the El Gamal key-generation is less compared to RSA. The second statement is correct, as the size of group elements used to instantiate ElGamal over the elliptic curves are very small compared to the size of group elements used to instantiate RSA over $\mathbb{Z}_N^\star$. The third statement is incorrect, as unlike RSA, for El Gamal scheme, it relatively safe if multiple receivers pick up the same group and same generator as their public parameters. The fourth statement is incorrect, as the scheme is CPA-secure under the DDH assumption. So the answers are **a** and **b**.

4. Consider the following modification to the Diffie-Hellman key-exchange protocol, executed over a cyclic group of order q with generator g: the sender and receiver send $K_s = g^x$ and $K_r = g^y$ to each other, where x, y are randomly selected from $\mathbb{Z}_q$ and outputs $K_s \cdot K_r$ as the final key. Assume DLog, CDH, DDH and all other related assumptions are true in the underlying group and this modified protocol is executed in the presence of a semi-honest PPT adversary. Then

   a. The adversary will completely know the underlying output key

   b. From the view point of the adversary, the output key is uniformly random and unknown

c. From the view point of the adversary, the output key will be pseudorandom

d. None of the above

Since adversary sees K_s and K_r as part of its transcript, it itself can compute the value $K_s \cdot K_r$, which is the output of the modified protocol and hence will completely know the output. So the answer is **a**.

5. Which of the following is/are correct with respect to the hybrid encryption scheme using KEM/DEM paradigm?

   a. If KEM is COA-secure and if we use a COA-secure Symmetric-Key encryption to encrypt the plaintext, then the overall hybrid scheme is CPA-secure

   b. The first component of the ciphertext produced by the hybrid encryption algorithm consists of an encryption of the symmetric key under the public key

   c. At the receiver end, two operations occur - a decapsulation operation, followed by a symmetric key encryption

   d. The Gen algorithm in KEM generates one key to be used in encryption of plaintext

   The first statement is correct as a combination of COA-secure KEM and a COA-secure SKE implies a CPA-secure hybrid scheme. The second statement is incorrect, as the first component consists of an encapsulation of the symmetric key and not its encryption. The third statement is incorrect as at the receiver end, two operations occur - a decapsulation operation, followed by a symmetric key decryption, and not encryption. The last statement is incorrect, as the Gen algorithm outputs two keys. So the answer is **a**.