DEALINE: To be submitted through the class rep latest Monday 19th October, 2020 at 5.00 p.m

BCT 2314 – ASSIGNMENT

1. Explain the working mechanisms of the below block ciphers
   a) Serpent (10 marks)
   b) IDEA (10 marks)
   c) CAST (10 marks)

BCT 2314 - CAT

1. What requirements must a public-key cryptosystems fulfill to be a secure algorithm? (4 marks)
2. Outline the components of the RSA algorithm (4 marks)
3. Let $(PU_a,\ PR_a)$ be the public and private key of Alice, and $(PU_b,\ PR_b)$ are the public and private key of Bob. Let $H()$ be a hash function, $E(Key, Data)$ denote an encryption, and $D(Key, Data)$ decryption operation, $||$ denotes a concatenation and Doc be a document. Describe the digital signature algorithm performed by Alice, on the document Doc. (5 marks)
4. Let $C(Key, M)$ denote a message authentication code function, produced for the message M and a shared key Key. Let $E(Key, M)$ denote encryption of a message M with a key Key, and let || denote the concatenation. If Alice send to Bob the following information: $E(K_2, M)||C(K_1, E(K_2, M))$ where K_1, K_2 are shared secret keys. Describe the goals of the message. (4 marks)
5. In the Diffie Hellman Key exchange protocol between user A and B both users have a private key: $X_A = 6$ and $X_B = 35$, respectively. The public keys are $Y_A = a^{X_A}\ mod\ p$ and $Y_B = a^{X_B}\ mod\ p$. What is the common key K for p = 71 and a = 7? (4 marks)
6. The RSA system was used to encrypt the message M into the cipher-text C = 6. The public key is given by $n = p.q = 187$ and $e = 107$. By answering the following, try to crack the system and to determine the original message M.
   a. What parameters comprises the public key and the private key? (2 marks)
   b. What steps are necessary to determine the private key from the public key? (2 marks)
   c. Determine the private key for the given system. (5 marks)
   d. What is the original message M? (2marks)
7. Recall the ElGamal cryptosystem. A community of users share a large prime p and a primitive element a. Each user has a key pair (x, Y), where $0 < x < p - 1$ is randomly chosen and $Y = a^x\ mod\ p$. Y is public and x is private. To send a message M to Alice, who has key pair $(x_A,\ Y_A)$, Bob performs the following steps:
   i. Choose a random x_B with $0 < x_B < p - 1$.
   ii. Compute $C_1 = a^{x_B}\ mod\ p$ and $C_2 = M.A^{x_B}\ mod\ p$
   iii. The ciphertext is (C_1, C_2).
   a. Explain how Alice decrypts the message, show the steps. (5 marks)

b. Assume that prime p = 17 and the primitive element a = 6. Bob, who has a private key $x_B = 12$ wants to send a message M = 5 to Alice, who has a public key $Y_A = 15$. Compute the ciphertext is (C_1, C_2). and show your steps. (5 marks)

9. A Feistel cipher is used in the DES algorithm.
   a. Describe the operation of a Feistel cipher. (5 marks)
   b. Briefly describe three modes of operation of DES. (5 marks)