BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION SYSTEMS

SECOND SEMESTER 2022-23
NETWORK SECURITY (CS G513)
COMPREHENSIVE EXAMINATION
(CLOSED BOOK)

Maximum Marks: 90
Time: 180 minutes

Instructions:

1. Answer all parts of a question together in the answer sheet. Answers at separate places will not be accepted.
2. Do not write any information irrelevant to the question.
3. Provide clear and relevant reasoning (wherever required) to support your answer.

Q.1. Answer the following:

a) The elements in a group do not have to be numbers or objects. They can be rules, mappings, functions, or even actions. Let us consider a very interesting group, that is, *permutation group*. This group is the set of all permutations for certain numbers and the operation is composition, i.e., applying one permutation after another. Each permutation is shown in table 1 in which the content shows where the input comes from, and the index defines the output. The composition involves applying two permutations, one after the other. The table shows how the operation is defined. The first row and column show the permutation and result is the corresponding cross-section element.

Table 1

	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 2 3]	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 3 2]	[1 3 2]	[1 2 3]	[2 3 1]	[2 1 3]	[3 2 1]	[3 1 2]
[2 1 3]	[2 1 3]	[3 1 2]	[1 2 3]	[3 2 1]	[1 3 2]	[2 3 1]
[2 3 1]	[2 3 1]	[3 2 1]	[1 3 2]	[3 1 2]	[1 2 3]	[2 1 3]
[3 1 2]	[3 1 2]	[2 1 3]	[3 2 1]	[1 2 3]	[2 3 1]	[1 3 2]
[3 2 1]	[3 2 1]	[2 3 1]	[3 1 2]	[1 3 2]	[2 1 3]	[1 2 3]

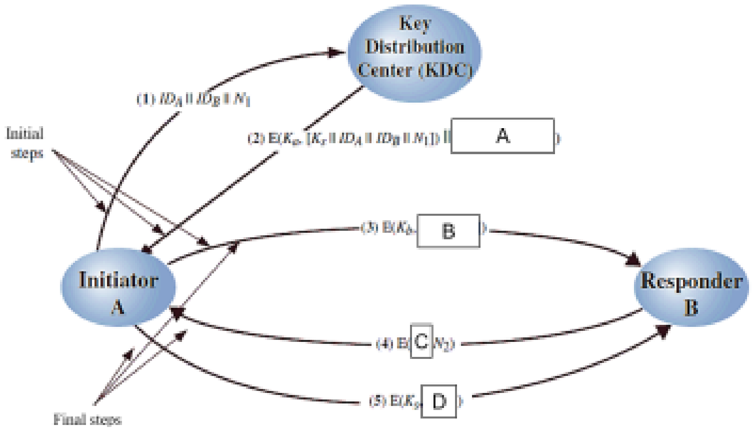
Considering the special set of permutations in table 1, write whether it forms a group? Provide the identity element of the group and inverse pairs for each element. Explain how group properties are satisfied/ not satisfied with reference to your answer. [9 M]

b) A subset H of a group G is a subgroup of G if H itself is a group with respect to the operation on G. For example, if G = <S, ○> is a group, H = <T, ○> is a group under the same operation, and T is a non-empty subset of S, then H is a subgroup of G. Explain whether the group H = <Z_{10}, +> is a subgroup of the group G = <Z_{12}, +>? Support your answer with a clear example and reasoning. [5 M]

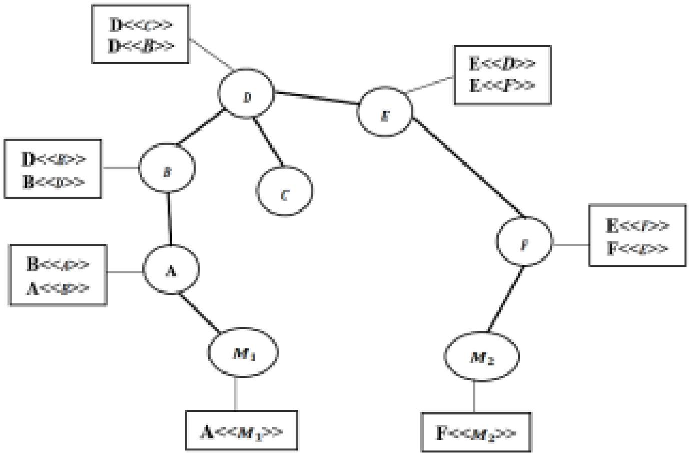
Q.2. Answer the following:

a) Two parties, A and B, agree to securely communicate using a shared secret key, K, exchanged with the help of Diffie-Hellman key exchange method. Both A and B, choose a prime number p, its primitive root g, and a hash function H. User A chooses a random number a and computes $M_1 \equiv g^a \bmod p$. For authentication purpose, A chooses a nonce N_A, and sends M_1 and N_A to B. While receiving M_1 and N_A, B computes $M_2 \equiv g^b \bmod p$ by choosing b as the random number. It also computes the hash of N_A as $H(N_A)$ and sends M_2, $H(N_A)$, and its own nonce N_B to A. Upon receiving M_2, $H(N_A)$, and N_B, A verifies the received hash $H(N_A)$ and computes the key as $K = (M_2)^a \bmod p$. It also computes the hash of N_B as $H(N_B)$ and sends it to B. Similarly, B computes the key as $K = (M_1)^b \bmod p$ and verifies the received hash $H(N_B)$. Consider an adversary, E, which intercepts all communication between A and B, and knows the parameters p and g. If E does not have any information about the hash function H, describe with proper reasoning whether it would be possible for E to get the secret key K and to establish the man-in-the-middle attack? Support your answer with clear and justified reasoning. [10 M]

b) Consider the below key distribution protocol. You are supposed to write the missing values labelled A, B, C, and D. [7 M]

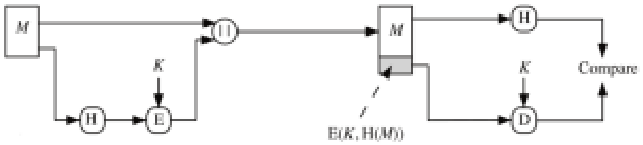

Key Distribution Center (KDC)
(1) $ID_A \| ID_B \| N_1$
(2) $E(K_a, [K_s \| ID_A \| ID_B \| N_1]) \|$ A)
Initial steps
(3) $E(K_b,$ B)
Initiator A
Responder B
(4) E(C N_2)
(5) $E(K_s,$ D)
Final steps

Q.3. Refer to the below X.509 hierarchy where certificate authorities are represented by *A, B, C, D, E,* and *F*, with two users M_1 and M_2. Suppose that user M_1 obtains the certificate of user M_2 and needs to process it so that M_2's public key can be retrieved. Considering the below hierarchy, explain whether user M_1 can obtain user M_2's public key? Support your answer with the help of CA<<user>> notion. [8 M]



Q.4. Answer the following:

a) Consider the mechanism illustrated below:



i) Which security service(s) the above mechanism provides? [2 M]

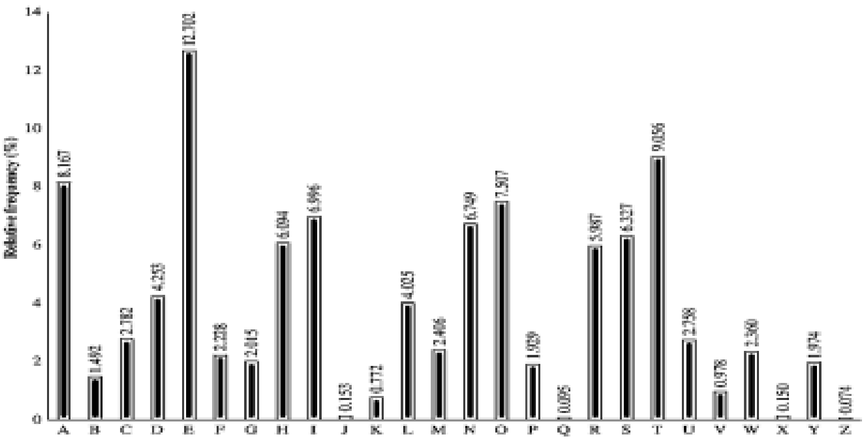
ii) What is second preimage resistant property? Explain how an attacker can defeat the above security service if the function *H*() does not have the second preimage resistant property. [4 M]

b) Consider group G of prime order p, a group generator g, and a group element h. Let a be an integer that you need to search in the range $[0, p\text{-}1]$ with the help of an integer r obtained by rounding up the square root of p. Given that it is possible to write a as a_0+ra_1 (a_0 and a_1 are randomly chosen integers) and that we have an equality between hg^{-a_0} and g^{ra_1} in group G. The below algorithmic code explains this concept by searching for a match between two lists of r elements each. The first list contains all group elements of the form hg^{-a_0} whereas the second list contains all group elements of the form g^{ra_1}. You are required to write what crypto-graphic criteria such formulation leads to using which we can perform a specific operation for h and g. Write the name of that specific operation and formulate your answer with clear reasoning. [12 M]

```
Algorithm
Require: A group $G$ of prime order $p$
Require: A group generator $g$ and a group element $h$
 $r \leftarrow \lceil \sqrt{p} \rceil$
 Create $T$ an array of $r$ group elements
 Create $I$ an array of $r$ integers
 $k \leftarrow h$
 for $i \leftarrow 0$ to $r-1$ do
   $T[i] \leftarrow k$ and $I[i] \leftarrow i$
   $k \leftarrow k/g$
 end for
 Sort $T$ and perform all exchanges simultaneously on $I$
 $k \leftarrow 1$
 $m \leftarrow g^r$ in $G$
 for $i \leftarrow 0$ to $r-1$ do
  Lookup $k$ in $T$ (using binary search)
  If $k$ is found at position $j$, return $ri + I[j]$
  $k \leftarrow k.m$ in $G$
 end for
```

Q.5. Recall the Monoalphabetic cipher, where a keystream is generated by jumbling the alphabetical sequence to get the random mapping, R. Such random mapping, R, is then used to encrypt the secret plaintext message M to get the ciphertext C. However, the plaintext message M can still be recovered from the ciphertext C if the cryptanalyst knows the nature of the plaintext. Information, such as, regularities of the underlying language with the help of mapping the letter-frequencies can be exploited to intelligently guess plaintext from cipher-text. Using this knowledge, you are required to cryptanalyze the below ciphertext, generated using the Mon-oalphabetic cipher for some jumbled sequence (secret key mapping). *Hint: English is used as the underlying language of the plaintext and its relative frequency distribution graph is given for your reference*. [13 M]

Ciphertext: A F F G G J F A D C G F Y



Q.6. Let us assume that a secure session and connection has been established between two parties (client and server) using SSL. The below information is stored by the client computer for this session/connection.

Session ID = *id*, Compression method = null, CipherSuite = TLS_DHE_RSA_WITH_AES_128_CBC_ SHA, Master secret = *s*, Server random = r_s, Client random = r_c, Server MAC secret = m_s, Client MAC secret = m_c, Server encrypt key = e_s, Client encrypt key = e_c.

a) Which algorithm/cipher is used by the client to authenticate the server? [2 M]

b) Write an equation that expresses SSL record operation on a single fragment *F* from client application that produces the packet to be sent *P*. Use the provided variables above and || for concatenate/append operator. For function names in equation you should use algorithm names (you cannot use E() for encrypt, H() for hash. Refer to specific algorithms). SSL header can be denoted as SSL. [6 M]

Q.7. Answer the following: [4 * 3 = 12 M]

a. Generate an element of the key stream using RC4 algorithm for a 4-byte example where $S = \{0, 1, 2, 3\}$, key = {1, 3, 5, 7}, and $i = j = 0$. Write computation steps and final value obtained as a key stream.

b. How are client and server mutually authenticated in Kerberos? Write the contents of the ticket and authenticator that client needs to provide when it reaches out to the target server.

c. What will happen if the decryptor is removed from polymorphic generator? Briefly explain any two polymorphic virus techniques used to avoid its detection.

[-- END OF QUESTION PAPER ------------------------------------]