

Birla Institute of Technology & Science, Pilani
Work Integrated Learning Programmes Division
First Semester 2023-2024,
Comprehensive Exam (EC-3 Regular)

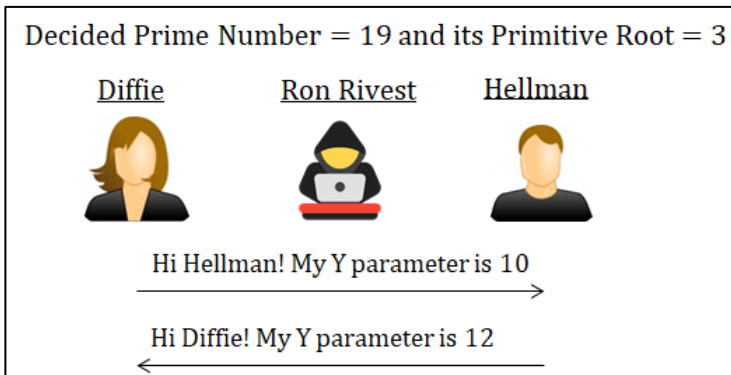
Course No. : CSI ZG513 / ES ZG513 / SS ZG513
Course Title : Network Security
Nature of Exam : Open Book
Weightage : 40%
Duration : X Hours
Date of Exam : 29/11/2024 (FN)

No. of Pages = 11
No. of Questions = 11x3 sets

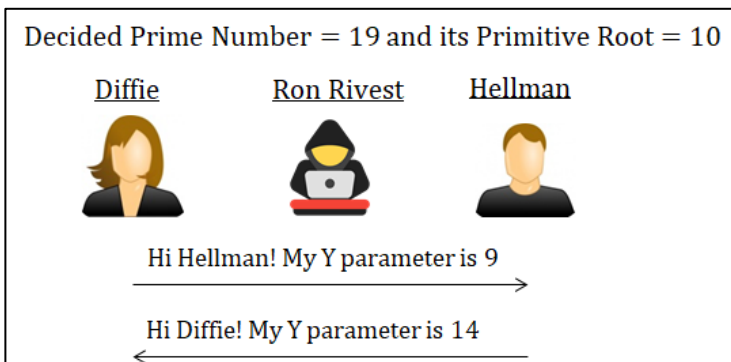
Note to Students:

1. Please follow all the *Instructions to Candidates* given on the cover page of the answer book.
2. All parts of a question should be answered consecutively. Each answer should start from a fresh page.
3. Assumptions made if any, should be stated clearly at the beginning of your answer.

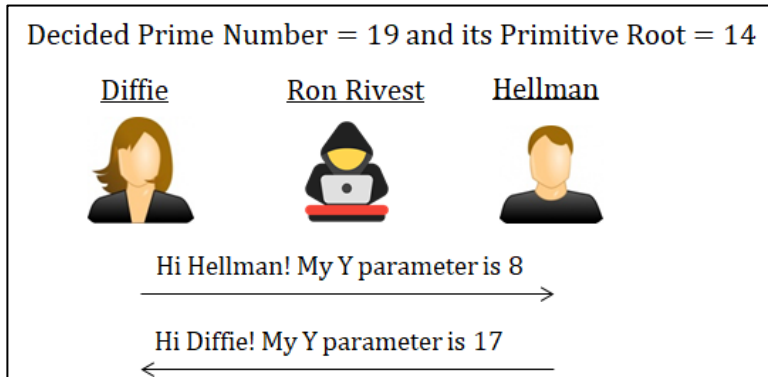
Q.1 Set. (A) Diffie and Hellman decided to exchange a secret key using Diffie-Hellman Key Exchange Algorithm. Show how the attacker Ron Rivest will be able to calculate the secret key if he is tapping all the messages. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions. **[3 Marks]**



Q.1 Set. (B) Diffie and Hellman decided to exchange a secret key using Diffie-Hellman Key Exchange Algorithm. Show how the attacker Ron Rivest will be able to calculate the secret key if he is tapping all the messages. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions. **[3 Marks]**



Q.1 Set. (C) Diffie and Hellman decided to exchange a secret key using Diffie-Hellman Key Exchange Algorithm. Show how the attacker Ron Rivest will be able to calculate the secret key if he is tapping all the messages. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions. **[3 Marks]**



Q.2 Set. (A) An anti-social group sent an ElGamal encrypted message to another one using the public key as $PU = \{p = 23, e_1 = 5, e_2 = 10\}$. You are an intelligent secret service agent and through earlier cryptanalysis you know that the last message it sent was decimal 15 in plaintext. You intercepted the cipher text for it as $\{C_1 = \text{Not Available}, C_2 = 21\}$ and subsequent message cipher text as $\{C_1 = 8, C_2 = 11\}$. Restore the plaintext for this second message taking the data (only) given in the situation. Justify your answer with all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions. **[3 Marks]**

Q.2 Set. (B) An anti-social group sent an ElGamal encrypted message to another one using the public key as $PU = \{p = 29, e_1 = 8, e_2 = 19\}$. You are an intelligent secret service agent and through earlier cryptanalysis you know that the last message it sent was decimal 17 in plaintext. You intercepted the cipher text for it as $\{C_1 = \text{Not Available}, C_2 = 26\}$ and subsequent message cipher text as $\{C_1 = 13, C_2 = 7\}$. Restore the plaintext for this second message taking the data (only) given in the situation. Justify your answer with all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions. **[3 Marks]**

Q.2 Set. (C) An anti-social group sent an ElGamal encrypted message to another one using the public key as $PU = \{p = 31, e_1 = 11, e_2 = 6\}$. You are an intelligent secret service agent and through earlier cryptanalysis you know that the last message it sent was decimal 15 in plaintext. You intercepted the cipher text for it as $\{C_1 = \text{Not Available}, C_2 = 28\}$ and subsequent message cipher text as $\{C_1 = 13, C_2 = 27\}$. Restore the plaintext for this second message taking the data (only) given in the situation. Justify your answer with all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions. **[3 Marks]**

Q.3 Set. (A) In the context of RSA, answer the following question. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions. **[3 Marks]**

I am a prime number p_1 . I am a prime number p_2 .

$(p_1 + p_2) = 500$ and $(p_1 - p_2) = 414$
 $n = p_1 * p_2$ and $e = 571$
So what is d ?

Q.3 Set. (B) In the context of RSA, answer the following question. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions. **[3 Marks]**

I am a prime number p_1 . I am a prime number p_2 .


$(p_1 + p_2) = 440$ and $(p_1 - p_2) = 306$
 $n = p_1 * p_2$ and $e = 571$
So what is d ?

Q.3 Set. (C) In the context of RSA, answer the following question. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions. **[3 Marks]**

I am a prime number p_1 . I am a prime number p_2 .

$(p_1 + p_2) = 360$ and $(p_1 - p_2) = 226$
 $n = p_1 * p_2$ and $e = 571$
So what is d ?

Q.4 Set. (A) Help the Network Security Engineer with calculations and justification. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions.
[3 Marks]




I am a Network Security Engineer.
Help me to select the better set for Blum-Blum-Shub PRNG.

Set-1: $n = 437, s = 11$

Set-2: $n = 517, s = 15$

Q.4 Set. (B) Help the Network Security Engineer with calculations and justification. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions.
[3 Marks]




I am a Network Security Engineer.
Help me to select the better set for Blum-Blum-Shub PRNG.

Set-1: $n = 209, s = 7$

Set-2: $n = 649, s = 21$

Q.4 Set. (C) Help the Network Security Engineer with calculations and justification. Direct answers or copy and paste from web/any tool will not be accepted. All notations are as explained in the lecture sessions.
[3 Marks]



I am a Network Security Engineer.
Help me to select the better set for Blum-Blum-Shub PRNG.

Set-1: $n = 1333, s = 67$

Set-2: $n = 1333, s = 83$

Q.5 Set. (A) A network engineer captured few hexadecimal bytes starting from Record Layer Protocol header as: 17 03 03 01 60 01... Answer the following questions in this context with proper and brief justification. Direct answers will not be accepted. Do not just write the byte values, state the meaning of it wherever required. **[3 Marks]**

- i. Which TLS sub-protocol is being carried by the Record Layer?
- ii. What is the TLS version used in the communication?
- iii. What is the content length? Answer in decimal.

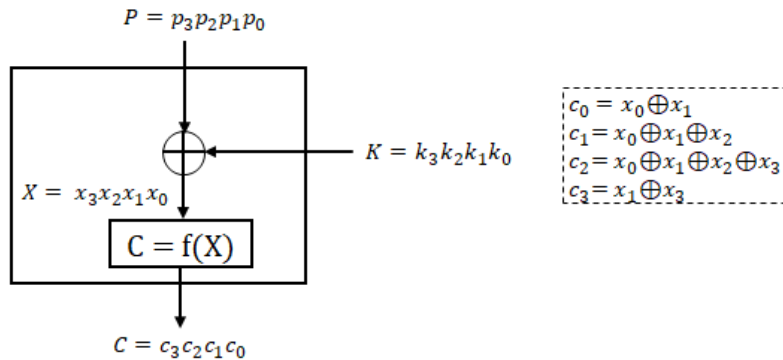
Q.5 Set. (B) A network engineer captured few hexadecimal bytes starting from Record Layer Protocol header as: 16 03 03 00 04 0E 00 00 00... Answer the following questions in this context with proper and brief justification. Direct answers will not be accepted. Do not just write the byte values, state the meaning of it wherever required. **[3 Marks]**

- i. Which TLS sub-protocol is being carried by the Record Layer?
- ii. What is the message? Explain its all details in brief.
- iii. Why the last three bytes are all 0s?

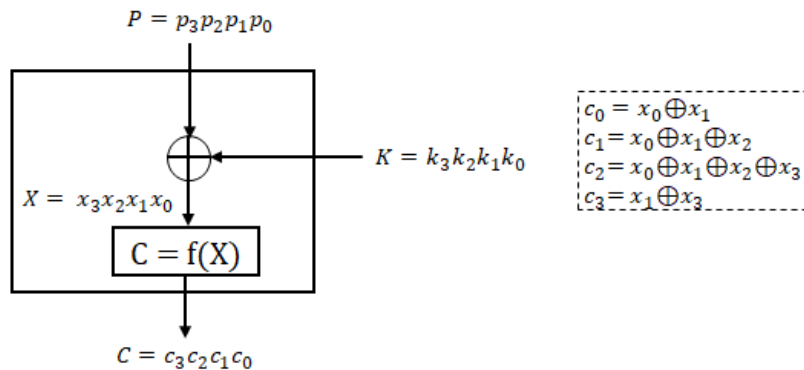
Q.5 Set. (C) A network engineer captured few hexadecimal bytes starting from Record Layer Protocol header as: 15 03 03 00 02 02 30. Answer the following questions in this context with proper and brief justification. Direct answers will not be accepted. Do not just write the byte values, state the meaning of it wherever required. **[3 Marks]**

- i. Which TLS sub-protocol is being carried by the Record Layer?
- ii. What is the message? Explain its all details in brief.
- iii. Do you think the content of the Record Layer encrypted? Why or why not?

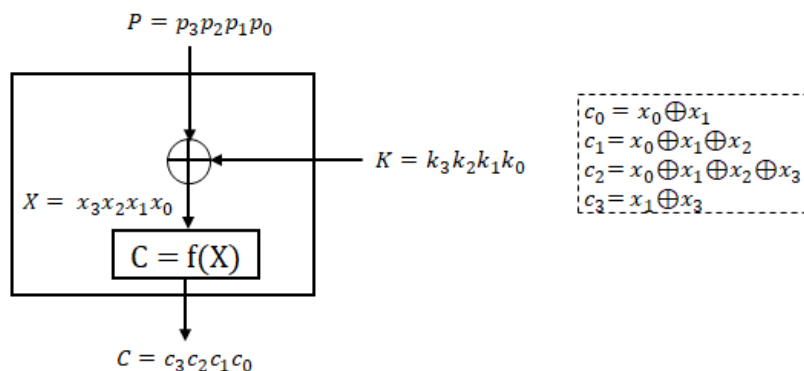
Q.6 Set. (A) Find out the ciphertext (C) in decimal form after applying the shown algorithm below. The decimal values of the plaintext (P) is 12 and the key (K) is 9. Each variable is also shown in four bits in the diagram. All other symbols carry their usual meanings. Show all the calculations. Direct answer will not secure any marks. [3 Marks]



Q.6 Set. (B) Find out the ciphertext (C) in decimal form after applying the shown algorithm below. The decimal values of the plaintext (P) is 15 and the key (K) is 12. Each variable is also shown in four bits in the diagram. All other symbols carry their usual meanings. Show all the calculations. Direct answer will not secure any marks. [3 Marks]



Q.6 Set. (C) Find out the ciphertext (C) in decimal form after applying the shown algorithm below. The decimal values of the plaintext (P) is 10 and the key (K) is 4. Each variable is also shown in four bits in the diagram. All other symbols carry their usual meanings. Show all the calculations. Direct answer will not secure any marks. [3 Marks]



Q.7 Set. (A) A message in ASCII is ***Hello***. SHA-512 has to be applied for calculating the hash code on this message. Show the first and the last 8 bytes in hexadecimal when this message is pre-processed as an input to the hash algorithm? Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. Character A in ASCII is 0x41 and a is 0x61. **[3 Marks]**

Q.7 Set. (B) A message in ASCII is ***Address***. SHA-512 has to be applied for calculating the hash code on this message. Show the first and the last 8 bytes in hexadecimal when this message is pre-processed as an input to the hash algorithm? Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. Character A in ASCII is 0x41 and a is 0x61. **[3 Marks]**

Q.7 Set. (C) A message in ASCII is ***Border***. SHA-512 has to be applied for calculating the hash code on this message. Show the first and the last 8 bytes in hexadecimal when this message is pre-processed as an input to the hash algorithm? Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. Character A in ASCII is 0x41 and a is 0x61. **[3 Marks]**

Q.8 Set. (A) During a diagnosis a network engineer captured the following hexadecimal bytes starting from an IP header: 45 00 00 B4 00 38 00 00 FF 33 A6 DC 0A 00 00 02 0A 00 00 01..... What is the size of source and destination IP addresses in bytes and what this IP datagram is carrying? Marks will be awarded only if the answers are technically justified. **[3 Marks]**

Q.8 Set. (B) During a diagnosis a network engineer captured the following hexadecimal bytes starting from an IP header: 60 00 00 00 00 a8 32 3f 20 03 00 51 60 12 00 00 00 00 00 00 00 00 02 20 03 00 51 60 12 00 00 00 00 00 00 00 00 04 3d 71 31 56..... What is the size of source and destination IP addresses in bytes and what this IP datagram is carrying? Marks will be awarded only if the answers are technically justified. **[3 Marks]**

Q.8 Set. (C) During a diagnosis a network engineer captured the following hexadecimal bytes starting from an IP header: 60 00 00 00 00 a8 33 3f 20 03 00 51 60 12 00 00 00 00 00 00 00 00 02 20 03 00 51 60 12 00 00 00 00 00 00 00 00 04 3d 71 31 56..... What is the size of source and destination IP addresses in bytes and what this IP datagram is carrying? Marks will be awarded only if the answers are technically justified. **[3 Marks]**

Q.9 Set. (A) The encryption key for the Hill Cipher is shown below. Case insensitive English text without space or any other extra character are prepared in 3x2 matrices in the column major order (a column is filled first). Decipher the message **ISAMZL**. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[3 Marks]**

$$\begin{bmatrix} 7 & 3 \\ 2 & 3 \end{bmatrix}$$

Q.9 Set. (B) The encryption key for the Hill Cipher is shown below. Case insensitive English text without space or any other extra character are prepared in 3x2 matrices in the column major order (a column is filled first). Decipher the message **IQDIGM**. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[3 Marks]**

$$\begin{bmatrix} 8 & 3 \\ 3 & 3 \end{bmatrix}$$

Q.9 Set. (C) The encryption key for the Hill Cipher is shown below. Case insensitive English text without space or any other extra character are prepared in 3x2 matrices in the column major order (a column is filled first). Decipher the message **ACPXUD**. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[3 Marks]**

$$\begin{bmatrix} 6 & 3 \\ 3 & 4 \end{bmatrix}$$

Q.10 Set. (A) In 64 bits DES, the input to the **first** four S-Boxes is 0xF1E2D3 (left to right). Find their output in hexadecimal showing necessary details. Direct answer will not secure any marks. **[3 Marks]**

Q.10 Set. (B) In 64 bits DES, the input to the **last** four S-Boxes is 0xF1E2D3 (left to right). Find their output in hexadecimal showing necessary details. Direct answer will not secure any marks. **[3 Marks]**

Q.10 Set. (C) In 64 bits DES, the input to the **middle** four S-Boxes is 0xF1E2D3 (left to right). Find their output in hexadecimal showing necessary details. Direct answer will not secure any marks. **[3 Marks]**

Q.11 Set. (A) Evaluate if the following statements are correct or not with proper reasoning in short. Unnecessary details will not be awarded any marks. Answers must be to the point. **[10 Marks]**

- i. It is not at all possible in TLS-1.2 that the length value of Record Protocol header is 4 and the length value of the Handshake Protocol header is 0.
- ii. Whichever protocol the TLS-1.2 Record Layer is carrying must also have a length field in its header otherwise the receiving end will not come to know about the length of the packet received.
- iii. In TLS-1.2, if the agreed upon cipher suite is TLS_RSA_WITH_NULL_SHA, it means the client and server will use RSA for encrypting the data and SHA with null initial value for calculating the hash code.
- iv. In TLS-1.2, if the length field of Handshake Protocol header is carrying a value X, then the length field of the Record Protocol header will be $(X - 4)$.

Q.11 Set. (B) Evaluate if the following statements are correct or not with proper reasoning in short. Unnecessary details will not be awarded any marks. Answers must be to the point. **[10 Marks]**

- i. In one TCP segment, only one TLS-1.2 Record Protocol header can appear, otherwise it will not be possible for the receiver TLS-1.2 layer to decipher the TLS security details.
- ii. TLS-1.2 provides encryption and authentication but the TLS-1.2 Alert Protocol messages are always visible to the IT administrators in plaintext, so that they can take corrective actions in case of fatal network errors.
- iii. In TLS-1.2, the internal clocks need to be set correctly at both client and server to use the 4 byte random number field for epoch, otherwise replay attacks cannot be detected.
- iv. In TLS-1.2 a man-in-the-middle cannot alter the offered cipher suites by the client to the server.

Q.11 Set. (C) Evaluate if the following statements are correct or not with proper reasoning in short. Unnecessary details will not be awarded any marks. Answers must be to the point. **[10 Marks]**

- i. In TLS-1.2, when a session is resumed, no pre-master secret will be generated. Only the sequence number which is used for MAC generation will be reset.
- ii. A client is communicating with a server using TLS-1.2 over TCP using anonymous Diffie-Hellman key exchange algorithm. The server will send the prime number and its primitive root through the certificate but the client will send the DH public parameters encrypted using the RSA algorithm.
- iii. In TLS-1.2 the content type field in the Record Protocol header must tell the web-server that HTTPS communication is going on, otherwise the web server will not be able to identify the type of type of traffic.
- iv. In TLS-1.2, a peer first needs to decrypt the incoming Record Layer packet to identify if it is a handshake, or alert or change_cipher_spec or application layer data.