الجامعة المستنصرية-كلية العلوم- قسم علوم الحاسوب- فرع الأمن السيبراني- الامتحان الأول- الأحد الموافق 26-03-2023

الاسم الثلاثي:

Q1) ANSWER THE FOLLOWING QUESTION:

1. What are the two keys involved in the Affine Cipher?
   a) Symmetric and asymmetric keys **b) Multiplicative and additive keys**
   c) Public and private keys d) None of the above
2. Which type of cipher is the Affine Cipher?
   a) Transposition cipher **b) Substitution cipher**
   c) Polyalphabetic cipher d) None of the above
3. What is cryptography?
   a. The practice of securing communication from authorized access.
   b. The practice of securing communication from third-party eavesdropping.
   c. The practice of securing communication from government surveillance.
   d. The practice of securing communication from internal threats.
4. What is a cryptosystem?
   a. The study of techniques used to break or weaken cryptographic systems.
   b. A secret value used to encrypt or decrypt messages.
   c. Combination of a cipher, key, and any related algorithms or protocols used to secure data.
   d. A method used to transform plaintext into ciphertext.
5. Which of the following is not a key role of cryptography in cybersecurity?
   a. Confidentiality. b. Integrity. c. Authentication. **d. Accessibility.**
6. What is non-repudiation?
   a. The process of transforming ciphertext back into plaintext.
   b. The study of techniques used to break or weaken cryptographic systems.
   c. A cryptanalysis technique where all possible keys are tried to decrypt a message.
   d. The process of ensuring that parties cannot deny their involvement in the exchange of information or transactions.
7. Which of the following is not a type of passive attack?
   a) Release of message contents b) Traffic analysis **c) Replay** d) All of the above
8. What is the goal of a passive attack?
   a) To modify the data stream b) To create a false stream
   c) To eavesdrop on or monitor transmissions d) To prevent the normal use of communications.
9. What does Denial of service attack do?
   a) Prevents or inhibits the normal use or management of communications facilities
   b) Alters the data stream c) Creates a false stream d) Masks the contents of messages
10. Cryptography helps ensure that sensitive information and communications are protected from unauthorized access, interception, or modification, providing _____. ANS: cybersecurity
11. Cryptography helps ensure that data is kept _____ and protected from unauthorized disclosure. ANS: secret

True/False:

1. Passive attacks are difficult to detect because they do not involve any alteration of the data. - **True**
2. Denial of service attack is a form of active attack. - **True**
3. Masquerade attack involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect. - **False** (This statement describes Replay attack, not Masquerade attack)
4. Passive attacks involve altering the data stream or creating a false stream. (**False**)

Q2) What are the three important principles that form the basis of information security and what do they refer to?
Answer:
Confidentiality refers to the protection of sensitive information from unauthorized access or disclosure. It involves ensuring that only authorized users have access to the information and that the information is protected from interception or eavesdropping during transmission.
Integrity refers to the protection of the accuracy and completeness of data and information. It involves ensuring that data is not altered or destroyed in an unauthorized or unintended manner and that the data remains consistent and accurate over time.
Availability refers to the assurance that data or information is genuine and can be trusted. It involves verifying the identity of the user or the source of the information and ensuring that the data has not been tampered with or modified.

Q3) Connect the situation or below description with the appropriate term (Cybersecurity, Network security, Data security, Information security) for the following:

ANSWER:

Cybersecurity	A government agency implements this type to protect against cyber threats, including cyber-attacks, cyber espionage, and cyber terrorism.
Network security	A bank implements this type to protect its computer networks from cyber-attacks and data breaches.
Data security	A healthcare organization implements this type to protect patient data, such as medical records, from being stolen or tampered with.
Information security	A company uses this type to protect its sensitive and confidential information from unauthorized access, disclosure, or theft.

Q4) Define "Security Service", List 3 TYPES ONLY of these services?

Answer: **Security Service:** a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. These services can be described as follow:
AUTHENTICATION, ACCESS CONTROL, DATA CONFIDENTIALITY,
DATA INTEGRITY, NONREPUDIATION, AVAILABILITY SERVICE

Q5) Find Greatest Common Divisor (GCD) for numbers 36 and -24?
Answer:
To find the GCD of two numbers, we need to find their common factors, both positive and negative, and then choose the greatest one.
First, we can find the factors of 36 and -24:
Factors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36 **AND** Factors of -24: -1, -2, -3, -4, -6, -8, -12, -24
The common factors are: 1, 2, 3, 4, 6, 12. Therefore, the GCD of 36 and -24 is also 12.

Q6) Let M= A mod N, use the modular exponentiation algorithm to compute M where A=-13, and N=5
Answer:

1. Convert the base number A to a non-negative integer a, such that a = A mod N and 0 <= a < N.
2. Convert the exponent to a binary number, e.g., 13 = 1101 (in binary).
3. Initialize a result variable, r, to 1.
4. For each bit of the exponent, starting from the least significant bit and moving left: a. Square the current value of r, i.e., r = r * r. b. If the current bit of the exponent is 1, multiply r by the base value a, i.e., r = r * a.
5. Return r mod N.

Using this algorithm, we can compute M = A mod N, where A = -13 and N = 5 as follows:

1. Convert A to a non-negative integer a: a = -13 mod 5 = 2.
2. Convert the exponent 1 to binary: 1 = 1 (in binary).
3. Initialize the result variable r to 1.
4. For the first bit of the exponent (which is 1): a. Square r: r = r * r = 1 * 1 = 1. b. Multiply r by a: r = r * a = 1 * 2 = 2.
5. Return r mod N: M = r mod N = 2 mod 5 = 2.

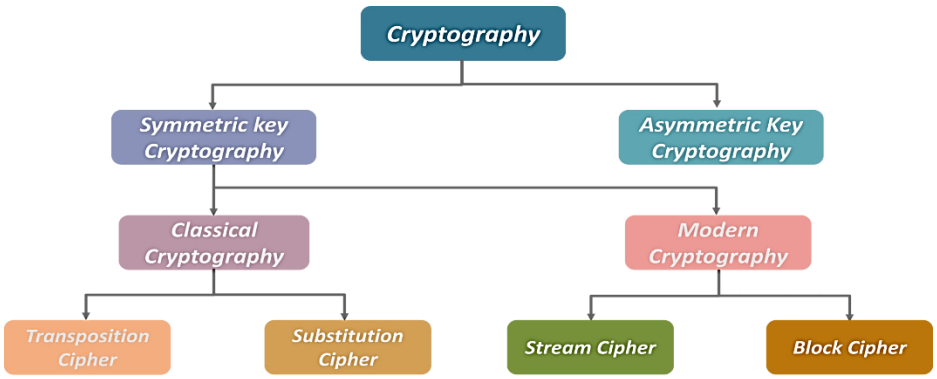
Therefore, the remainder when -13 is divided by 5 is 2, and M = 2.

Q7) Compute $\phi(n) = n \prod_{\substack{p|n \\ \text{p prime}}} \left(1 - \frac{1}{p}\right)$ **, where n=15?**

ANSWER:

$$\begin{aligned} \phi(15) &= 15 \prod_{\substack{p|15 \\ \text{p prime}}} \left(1 - \frac{1}{p}\right) \\ &= 15 \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{5}\right) \\ &= 8 \end{aligned}$$

Q8) Describe using FIGURE only the framework of Cryptography classification?
ANSWER:



Q9) Encrypt Plaintext= "**MUSTANSIRIYAH**" with Keyword="**TOYOTA**", using Playfair Encryption method?
ANSWER:

Playfair square

T	O	Y	A	B
C	D	E	F	G
H	I	K	L	M
N	P	Q	R	S
U	V	W	X	Z

Transformed text
HZNBTRPMPLABLU

KEYWORD=TOYA; P=MU ST AN SI RI YA HX
MU=HZ
ST=NB
AN=TR....
HX=LU

Q10) Decrypt Ciphertext= **"NQO"** with a^-1=21 AND b=8, using Affine Cipher method?
ANSWER:
LET ALPHABET:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plain Text = (**a^-1** * (C - b)) mod 26, so the **a^-1** =21 , AND b=8

P(N) =(21*(13-8))MOD 26=105 MOD 26= 1 =**B**
P(Q) =(21*(16-8))MOD 26=168 MOD 26= 12 =**M**
P(O) =(21*(14-8))MOD 26=126 MOD 26= 12 =**W**