Question 1.

Part a (Question). List and briefly define categories of passive and active security attacks.

Part a (Answer).

Active attacks involve some modification of the data stream or the creation of a false stream, and can be subdivided into four categories, i.e., masquerade, replay, modification of messages, and denial of service.

- **Masquerade:** An attacker pretends to be an authorized user in a system.
- **Replay:** An attacker captures messages transmitted from sender(s) to receiver(s) and then replays the captured message to receiver(s).
- **Modification of a message:** Some portion of a legitimate message is altered or a set of messages are reordered or delayed by an attacker.
- **Denial of service:** An attacker attempts to prevent legitimate users from accessing the service.

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. There are two types of passive attacks, i.e., release of message contents and traffic analysis.

- **Release of message contents**: An attacker attempts to learn the contents that is being transmitted, such as a telephone conversion, an electronic mail message and a transferred file etc.
- **Traffic analysis:** An attacker tries to learn the pattern of the transmitted message including the location and identity of the communication host, as well as the frequency and length of messages being exchanged.

Part b (Question). List and briefly define the basic security requirements in computer and network security.

Part b (Answer).

The security requirements fall in two main categories:

- **Functional requirements**
- **Assurance requirements**

By the way, essential computer and network security requirements can be enumerated as bellow:

- **Accountability:** Assure the traceability of actions, which is performed on a system to a specific system entity (user, process, and device).
- **Availability:** Assure that systems work promptly and service is not denied to authorized users.
- **Authenticity:** The property of being genuine and being able to be verified and trusted.
- **Integrity (Data and System Integrity):** Assure that information are changed only in a specific and authorized manner and the system performs its intended function in an unimpaired (strong and stable) manner.
- **Confidentiality (Data confidentiality and privacy):** Assure that private or confidential information is not made available or disclosed to unauthorized individuals.

And network security services can be listed as follows:

- **Authentication**: Assure that a communication is authentic. For example, assure the recipient that the message is from the source that it claims to be from.
- **Access Control**: Control and limit the access to host systems and applications via communications links.
- **Data Confidentiality**: Protect transmitted data from passive attacks.
- **Data Integrity**: Protect transmitted data from active attacks.
- **Non-Repudiation**: Prevent either sender or receiver from denying a transmitted message.
- **Availability Service**: Assure that a system is accessible and usable upon.

Part c (Question). Describe the Kerckhoffs's Principles.

Part c (Answer).

Based on Kerckhoffs's principles, in designing a cryptosystem we need to guarantee that a cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

1. The system must be substantial, if not mathematical, undecipherable;
2. The system must not require secrecy and can be stolen by the enemy;
3. The system must be easy to communicate and remember the key without using requiring written notes, and it must also be easy to change or modify the keys with different participants;
4. The system ought to be compatible with telegraph communication;
5. The system must be portable, and its use must not require more than one person;
6. Finally, regarding the circumstances in which such system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.

Part d (Question). Describe the functions of confusion and diffusion in symmetric ciphers.

Part d (Answer).

- **Confusion**: Process of substituting characters or symbols to make the relationship between ciphertext and key as complex as possible.
- **Diffusion**: Process of spreading effect of plaintext or key as widely as possible over ciphertext and dispersing the effect of individual key or message bits over the plaintext. For example, little change in input stream or key will cause a big change in output.

Part e (Question). Describe the Strict Avalanche Conditions in symmetric ciphers.

Part e (Answer).

Each $m * n$ S-Box is a basic component in Symmetric-key algorithms and transforms the input bits (m bit) into output bits (n bit) by an implemented lookup table. The substitution algorithm should have good avalanche properties.

Strict Avalanche Criterion (SAC): State that any output bit j of an S-Box should change with probability $\frac{1}{2}$ when any single input bit i is inverted for all i, j.

Bit Independence Criterion (BIC): State that output bits j and k should change independently when any single input bit i is inverted for all i, j and k.

Part f. (Question). Describe the key management problem in conventional cryptosystems.

Part f (Answer).

A cryptosystem has at least five important entities: 1) Plaintext, 2) Secret Key, 3) Ciphertext, 4) Encryption Algorithm and 5) Decryption Algorithm. Key management is a critical part in both symmetric and asymmetric cryptosystems. In a symmetric encryption algorithm, the encryption key is identical to decryption key, while two distinct keys are used in an asymmetric encryption algorithm, i.e., public key and secret key. Key management typically consists of four steps for carefully dealing with the key generation, key exchange, key storage, key usage, key crypto-shredding (destruction) and key replacement:

- **Key Generation**: Key is generated according to the security parameters.
- **Key Exchange**: Before making a secure communication, key must be exchanged between communication entities (sender and receiver).
- **Key Storage**: Key must be saved and stored securely.
- **Key Lifetime**: Manage the key usage period and the key replacement frequency.

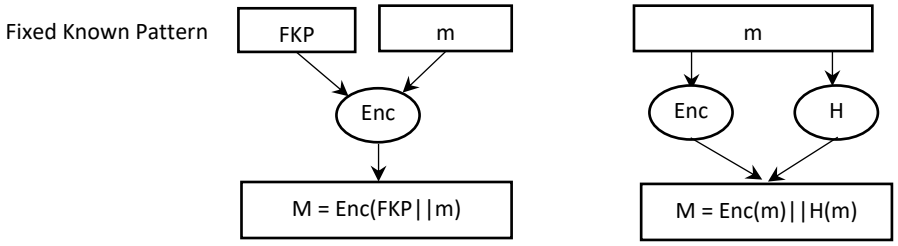
Question 2.

A fundamental cryptographic principle states that all messages must have redundancy. But we also know that redundancy helps an intruder tell if a guessed key is correct. Consider two forms of redundancy. First, the initial n bits of the plaintext contain a known pattern. Second, the final n bits of the message contain a hash over the message. From a security point of view, are these two equivalent? Discuss your answer.

Answer.

There are two fundamental cryptographic principles:

- **Redundancy**: Message must contain some redundancy to prevent intruders from sending garbage message and tricking the receiver.
- **Freshness**: Some method is needed to foil replay attacks, which is a basic cryptographic principle.



In this question two different approaches have been proposed to satisfy redundancy. If we doesn't have any detail of the cryptosystem and try only by generating different permutation based on the given plaintext both of them are hard to recover plaintext m or guess the key. But as the second one has operated by adding n-randomly series of bits, it is more secure than the first one that has operated by adding n-fixed known pattern. If intruder finds the fixed known plaintext, he/she can use it to recover the message, because he/she has some portion of the message. And also in the second approach intruder faces with two different algorithm, encryption/decryption algorithm and hash algorithm. In contrast to the fixed known pattern, hash algorithm generates the random output with different mechanism ad it is much harder to detect or predict the behavior.

Question 3.

Suppose that a message has been encrypted using DES in ciphertext block chaining mode. One bit of ciphertext in block C_i is accidentally transformed from a 0 to a 1 during transmission. How much plaintext will be garbled as a result?

Answer.

Consider 5 ciphertext C_1, C_2, … and C_5. If we have had a problem in C_2, only P_2 and P_3 would be garbled.

$P_1 = Dec_K(C_1)$ xor C_0; C_0 = Initialization Vector (IV).

$P_2 = Dec_K(C_2)$ xor C_1; C_2 with transmission error, will affect P_2.

$P_3 = Dec_K(C_3)$ xor C_2; C_2 with transmission error, will affect P_3.

$P_4 = Dec_K(C_4)$ xor C_3

$P_5 = Dec_K(C_5)$ xor C_4

Therefore, existing an error in C_k will only affect P_k and P_{k+1}.

Question 4.

The following is a ciphertext with Caesar Cipher, please analyze it, and give the corresponding plaintext and the used key.

DRO MSDI LBSWC GSDR CEWWOB'C NOVSQRDC, GSDR MYVYBPEV ZBYNEMO SX DRO WKBUOD CDKXNC KXN RKGKSSKX WECSM CZSVVSXQ YXDY LOKMROC.

Answer.

We can create different substitutions of alphabet letters by shifting 0 to 25.

For example, the first word of ciphertext (**DRO**) has 26 different cases by n-shifting algorithm.

0DRO,1ESP,2FTQ,3GUR,4HVS,5IWT,6JXU,7KYV,8LZW,9MAX,10NBY,11OCZ,12PDA,13QEB,14RFC,15SGD,**16THE**,17UIF,18VJG,19WKH,20XLI,21YMJ,22ZNK,23AOL,24BPM,25CQN

Based on the relative frequency, 'e' is the most popular in plaintext and 'o' is the most popular in this Caesar cipher, so we can assume o→e, then use the relation to check others.

Finally, this Caesar cipher has been made by shift 26-16+1=11. (A→K, B→L, C→M, D→N, E→O, F→P . . .)

Plaintext: **THE CITY BRIMS WITH SUMMER'S DELIGHTS, WITH COLORFUL PRODUCE IN THE MARKET STANDS AND HAWAIIAN MUSIC SPILLING ONTO BEACHES.**

Question 5.

Please complete the following two tables, and describe why Z_{11} and Z_{11}^* are abelian groups.

Answer.

x + y mod 11	x = 0	1	2	3	4	5	6	7	8	9	10
y = 0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

- **Closure:** result of operation (x + y) mod 11 is in set Z_{11}.
- **Associativity:** x + (y + z) mod 11 = (x + y) + z mod 11
- **Existence of identity:** When e = 0, e + x = x + e = x mod 11 for each x in Z_{11} holds. Thus, e = 0 is the identity.
- **Existence of inverse:** For each x in Z_{11}, it has inverse x^{-1}=11-x, because $x + x^{-1} = x^{-1} + x = e$;
- **Commutativity:** (x + y) mod 11 = (y + x) mod 11.

x * y mod 11	x = 1	2	3	4	5	6	7	8	9	10
y = 1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

- **Closure:** result of operation (x*y mod 11) is in set Z_{11}^*.
- **Associativity:** x*(y*z) mod 11 = (x*y)*z mod 11
- **Existence of identity:** When e = 1, e*x=x*e=x mod 11 for each x in Z_{11}^* holds. Thus, e=1 is the identity.
- **Existence of inverse:** For each x in Z_{11}^*; x has an inverse which is shadowed in table.
- **Commutativity:** x*y mod 11=y*x mod 11.

Question 6.

Prove the following:

(a) [(a mod n) + (b mod n)] mod n = (a + b) mod n

(b) [(a mod n) × (b mod n)] mod n = (a × b) mod n

Answer.

Part a)

Assume a mod n = p, then $a = nk_1 + p$

Assume b mod n = q, then $b = nk_2 + q$

Left side: [(a mod n) + (b mod n)] mod n = p + q mod n

Right side: a + b mod n = $[(nk_1 + p) + (nk_2 + q)]$ mod n = $[n(k_1 + k_2) + p + q]$ mod n = p + q mod n

Thus, [(a mod n) + (b mod n)] mod n = (a + b) mod n

Part b)

Assume a mod n = p, then $a = nk_1 + p$

Assume b mod n = q, then $b = nk_2 + q$

Left side: [(a mod n) * (b mod n)] mod n = p * q mod n

Right side: a * b mod n = $[(nk_1 + p) * (nk_2 + q)]$ mod n = $[n(k_1k_2+k_1q+k_2p) + p * q]$ mod n = p * q mod

Thus, [(a mod n) × (b mod n)] mod n = (a × b) mod n

Question 7.

Prove the following:

a) Prove the One-time padding is provably secure.

b) Prove the Fermat's Little Theorem $a^{p-1} \equiv 1$ mod p, where p is prime and gcd(a, p) = 1.

c) Prove that there are infinitely many primes.

Answer.

Part a)

The probability of a plaintext bit being 0 or 1 is not equal, i.e., P(bitP=0) = x and P(bitP=1) = 1-x
The probability of a key bit being 0 or 1 is equal, P(bitK=0) = ½, (bitK=1) = ½.
The Probability of a chipertext bit can be calculated as bellow.

Plaintext		Key		Ciphertext (XOR operation)	
p values	P(p)	k values	P(k)	c values	P(c)
0	x	0	½	0	x*½
0	x	1	½	1	x*½
1	1-x	0	½	1	(1-x)*½
1	1-x	1	½	0	(1-x)*½
P(c=0) = x*½ + (1-x)*½ = ½; P(c=1) = x*½ + (1-x)*½ = ½;					

Thus, the One-time padding is secure.

Part b)

Suppose that $Z_p^* = \{1, 2, 3, \cdots, p-1\}$ and $\mathrm{B} = \{\mathrm{a} * 1, \mathrm{a} * 2, \mathrm{a} * 3, \cdots, \mathrm{a} * (\mathrm{p}-1)\}$ for any $\mathrm{a} \in Z_p^*$. we need to prove $|Z_p^*| = |B|$ or there is not redundant element in B, so the p-1 multiples of a in B are distinct and nonzero.
By contradiction, if $i \neq j$, $\mathrm{a} * i = a * j \bmod p$
If $\mathrm{a} * i = a * j \bmod p$, $\mathrm{a} * (i-j) = 0 \bmod p$. Then, $\mathrm{a} = 0 \bmod p$ or $i - j = 0 \bmod p$.
As we know that $\gcd(\mathrm{a}, \mathrm{p}) = 1$, thus $\mathrm{a} \neq 0 \bmod p$ and $i - j = 0 \bmod p$. Then, $i = j$
Now we know that $|Z_p^*|$ and $|B|$ have the same number of elements, and try to calculate the multiplication of element in Z_p^* and B.
$\prod_{x_i \in Z_p^*} x_i = \prod_{x_i \in Z_p^*} a * x_i \bmod p$.
$\prod_{x_i \in Z_p^*} x_i = 1 * 2 * 3 * \cdots * (p-1) \bmod p$.
$\prod_{x_i \in Z_p^*} a * x_i = (a*1) * (a*2) * (a*3) * \cdots * \big(a * (p-1)\big) \bmod p = a^{p-1}\big(1 * 2 * 3 \cdots * (p-1)\big) \bmod p$.
Assume that $1 * 2 * 3 * \cdots * (p-1) \bmod p = \alpha$.
Then, $\alpha \bmod p = a^{p-1} * \alpha \bmod p$, so $(a^{p-1} - 1) * \alpha \bmod p = 0 \bmod p$.
Thus, $a^{p-1} = 1 \bmod p$.

Part c)

Assume that the primes are finite, and we can list them as $L = \{p_1, p_2, p_3, \cdots, p_r\}$.
Let P be any common multiple of these primes plus one, i.e., $P = p_1 * p_2 * p_3 * \cdots * p_r + 1$. Then, P is either a prime or not.
If P is a prime, then P is a new prime that was not in L and therefore we cannot say L is finite.
If P is not prime, then P is devisable by some prime call α.
$\alpha | P$ and as we assume that L is finite and α is in L, then $\alpha | p_1 * p_2 * p_3 * \cdots * p_r$.
$\alpha | p_1 * p_2 * p_3 * \cdots * p_r + 1$ and $\alpha | p_1 * p_2 * p_3 * \cdots * p_r$, then $\alpha | (p_1 * p_2 * p_3 * \cdots * p_r + 1 - p_1 * p_2 * p_3 * \cdots * p_r$.
Thus, $\alpha | 1$ and it is impossible. So α cannot divide P and therefore P is a new prime that was not in L.
Therefore, the primes are infinite.

Question 8.

Using the extended Euclidean algorithm, find the multiplicative inverse of
a) 1234 mod 4321
b) 550 mod 1769

Answer.

Part a)

Dividend	Divisor	Quotient	Reminder
4321	1234	3	619
1234	619	1	615
619	615	1	4
615	4	153	3
4	3	1	1

1) 1 = 4 – (3 * 1) = 4 – 3 * 1
2) 1 = 4 – (615 - 4 * 153) * 1 = 4 * 154 – 615
3) 1 = (619 – 615 * 1) * 154 – 615 = 619 * 154 – 615 * 155
4) 1 = 619 * 154 - (1234 – 619 * 1) * 155 = 619 * 309 – 155 * 1234
5) 1= (4321 – 1234 * 3) * 309 – 155 * 1234 = 4321 * 3090 – 1234 * 1082

➔ 4321 * 309 + 1234 * (-1082) = 1 mod 4321
➔ 1234 * (-1082) = 1 mod 4321
➔ -1082 mod 4321 = 4321 – 1082 = 3239 → $(1234)^{-1}$ mod 4321 = **3239**

Part b)

Dividend	Divisor	Quotient	Reminder
1769	550	3	119
550	119	4	74
119	74	1	45
74	45	1	29
45	29	1	16
29	16	1	13
16	13	1	3
13	3	4	1

1) 1 = 13 – 3 * 4 = 13 – (16 – 13 * 1) * 4 = 13 * 5 – 16 * 4
2) 1 = (29 – 16 * 1) * 5 – 16 * 4 = 29 * 5)– 16 * 9
3) 1 = 29 * 5 – (45 – 29 * 1) * 9 = 29 * 14 – 45 * 9
4) 1 = (74 – 45 * 1) * 14 – 45 * 9 = 74 * 14 – 23 * 45
5) 1 = 74 * 14)– 23 * (119 – 74 * 1) = 37 * 74 – 119 * 23
6) 1 = 37 * (550 – 119 * 4) – 119 * 23 = 37 * 550 – 171 * 119
7) 1= 37 * 550 – 171 * (1769 – 550 * 3) = 550 * 550 – 171 * 1769

➔ 1769 * (171) – 550 * (550) = 1 mod 1769
➔ 550 * (550) = 1 mod 1769
➔ +550 mod 1769 = 550 → $(550)^{-1}$ mod 1769 = **550**

Question 9.

Suppose Alice and Bob shared the common modulus n=p*q=35263, but have different public-private key pairs (e_1=17, d1) and (e_2=23, d2). If David wants to send a message M to Alice and Bob, he first computes the cipher text $C_1=M^{e1}$ mod n for Alice, the value of C_1 is 28657, and also compute the cipher text $C_2=M^{e2}$ mod n for Bob, the value of C_2 is 22520. Finally, David send (C_1, C_2) to Alice and Bob, respectively. Now, suppose a passive adversary A eavesdrops the cipher-texts (C_1, C_2). Can the adversary A recover message M just from (C_1, C_2) and then public keys (n, e_1, e_2)? If the adversary A can. Please show what strategy that the adversary A would apply, and give the value of message M as well.

Answer.

As we mentioned in the class, in this situation, the RSA could be unsecure, and the attacker could be able to recover the message M.

We know $C_1 = M^{e_1} \ mod \ n$ and $C_2 = \mathrm{M}^{e_2} \ mod \ n$; by assuming $e_1u + e_2v = 1$, try to calculate ${C_1}^u * {C_2}^v = (M^{e_1})^u * (\mathrm{M}^{e_2})^v = M^{e_1u+e_2v} = M \ mod \ n$. Hence, we only need to solve $e_1u + e_2v = 1$, by applying Extended Euclidian algorithm.

$pk_1 = (e_1, n) = (17, 35263) \rightarrow C_1 = 28657 = M^{17} \; mod \; 35263$
$pk_2 = (e_2, n) = (23, 35263) \rightarrow C_2 = 22520 = M^{23} \; mod \; 35263$
$C_1{}^{u} * C_2{}^{v} = ((M^{17})^{u}) * ((M^{23})^{v}) = M^{17u+23v} \; mod \; 35263 \xrightarrow{17u+23v=1} = M$
$17u + 23v = 1 \xrightarrow{Extended \; Euclidian \; Alg.} 17(-4) + 23(3) = -68 + 69 = 1 \rightarrow u = -4 \; and \; v = 3$
$C_1{}^{-4} * C_2{}^{3} = (C_1{}^{-1})^4 * (C_2{}^{3}) = (28657^{-1})^4 * (22520)^3 \; mod \; 35263 \xrightarrow{(28657)^{-1} mod \; 35263 = 34884}$
$34884^4 * 22520^3 mod \; 35263 = 168 \rightarrow m = 168$