FACULTY OF COMPUTER SCIENCE
CS4355: Cryptanalysis an DB Security
Professor: Dr. Rongxing Lu
Office: GE 114
Email: rlu1@unb.ca
Phone: 451-6966
Fall 2019 Tutorial Time: T 2:30-3:20

Tutorial 1

1) Briefly define essential computer and network security requirements including Accountability, Availability, Authenticity, Integrity, Confidentiality.
   - Answer:
     - Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
     - Availability: Assures 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; confidence in the validly of a transmission, a message, or a message originator.
     - Data integrity: assures that information and programs are changed only in a specified authorized manner system integrity: assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
     - Data confidentiality: assures that private or confidential information is not made available or disclosed to unauthorized individuals; Privacy: assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
2) Briefly define the Caesar cipher.
   - Answer: The Caesar cipher involves replacing each letter of the alphabet with the letter standing k places further down the alphabet, for k in the range 1 through 25.
3) What is the difference between passive and active security attacks?
   - Answer: Passive attacks have to do with eavesdropping on, or monitoring, transmissions. Electronic mail, file transfers, and client/server exchanges are examples of transmissions that can be monitored. Active attacks include the modification of transmitted data and attempts to gain unauthorized access to computer systems.
     Passive attacks: release of message contents and traffic analysis. Active attacks: masquerade, replay, modification of messages, and denial of service.
4) What is the Denial of Service (DoS) attack?
   - Answer: Denial of Service (DoS): prevents the normal use or management of communications facilities. DoS attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of DoS is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.
5) What is the non-repudiation?
   - Answer: Nonrepudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
6) A generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: For each plaintext letter p, substitute the ciphertext letter C:

$$C = E([a, b], p) = (ap + b) \bmod 26$$

   A basic requirement of any encryption algorithm is that it be one-to-one. That is, if $p \neq q$, then $E(k, p) \neq E(k, q)$. Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for $a = 2$ and $b = 3$, then $E([a, b], 0) = E([a, b], 13) = 3$.
   - Are there any limitations on the value of b? Explain why or why not.
     - Answer: No. A change in the value of b shifts the relationship between plaintext letters and ciphertext letters to the left or right uniformly, so that if the mapping is one-to-one it remains one-to-one.
   - Determine which values of a are not allowed.
     - Answer: $2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24$. Any value of a larger than 25 is equivalent to $a \bmod 26$.

- Provide a general statement of which values of a are and are not allowed. Justify your statement.
  - Answer: The values of a and 26 must have no common positive integer factor other than 1. This is equivalent to saying that a and 26 are relatively prime, or that the greatest common divisor of a and 26 is 1. To see this, first note that $E(a, p) = E(a, q)$ $(0 \leq p \leq q < 26)$ if and only if $a(p - q)$ is divisible by 26.
    1. Suppose that a and 26 are relatively prime. Then, $a(p - q)$ is not divisible by 26, because there is no way to reduce the fraction $a/26$, and $(p - q)$ is less than 26.
    2. Suppose that a and 26 have a common factor $k > 1$. Then $E(a, p) = E(a, q)$, if $q = p + m/k \neq p$ where $m = 26$.

7) A ciphertext has been generated with an affine cipher. The most frequent letter of the ciphertext is "B", and the second most frequent letter of the ciphertext is "U". Break this code.
   - Answer: Assume that the most frequent plaintext letter is e and the second most frequent letter is t. Note that the numerical values are $e = 4; B = 1; t = 19; U = 20$. Then we have the following equations:

$$1 = (4a + b) \bmod 26, \qquad 20 = (19a + b) \bmod 26$$

   Thus, $19 = 15a \bmod 26$. By trial and error, we solve: $a = 3$. Then $1 = (12 + b) \bmod 26$. By observation, $b = 15$.

8) Using the Vigenre cipher, encrypt the word "explanation" using the key "leg".
   - Answer:

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

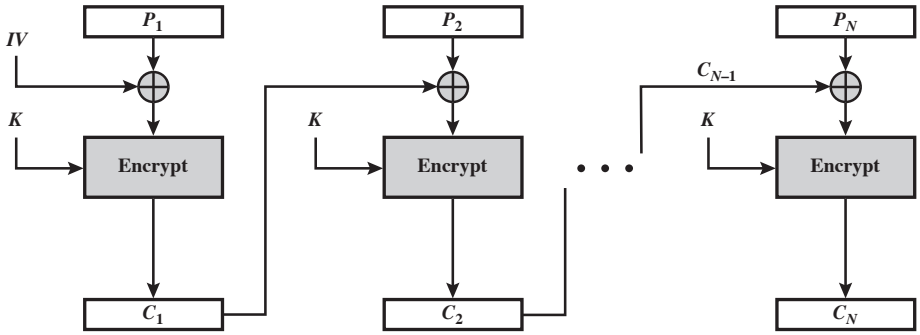
Plain text	e	x	p	l	a	n	a	t	i	o	n
key	l	e	g	l	e	g	l	e	g	l	e
Cipher text	p	b	v	w	e	t	l	x	o	z	r

Tutorial 2

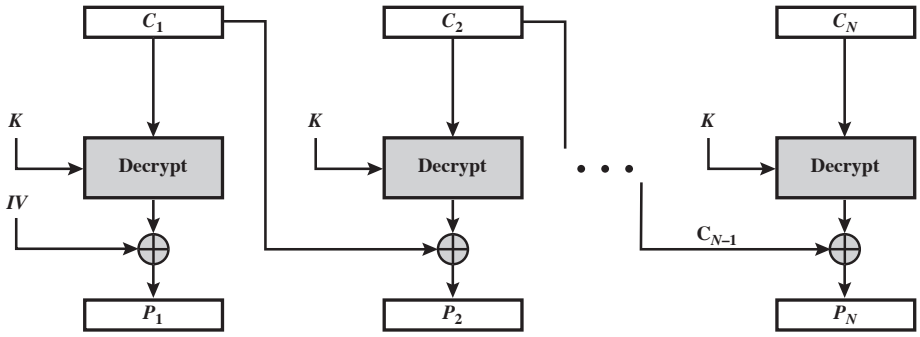
1) What is the difference between a block cipher and a stream cipher?
   - Answer: A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
2) What is the difference between diffusion and confusion?
   - Answer: In diffusion, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits, which is equivalent to saying that each ciphertext digit is affected by many plaintext digits. Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key. Thus, even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key. This is achieved by the use of a complex substitution algorithm.
3) Explain the avalanche effect.
   - Answer: The avalanche effect is a property of any encryption algorithm such that a small change in either the plaintext or the key produces a significant change in the ciphertext.
4) Prove One-Time Padding is unconditional secure.
   - Answer: The security depends on the randomness of the key, but it is hard to define randomness. In cryptographic context, we seek two fundamental properties in a binary random key sequence: **Unpredictability:** Independent of the number of the bits of a sequence observed, the probability of guessing the next bit is not better than 1/2. Therefore, the probability of a certain bit being 1 or 0 is exactly equal to 1/2. **Balanced (Equal Distribution):** The number of 1 and 0 should be equal.

m_i	Prob. m	k_i	Prob. k	c_i	Prob. c
0	x	0	$1/2$	0	$x/2$
0	x	1	$1/2$	1	$x/2$
1	$1-x$	0	$1/2$	1	$(1-x)/2$
1	$1-x$	1	$1/2$	0	$(1-x)/2$

   The probability of a key bit being 1 or 0 is exactly equal to $1/2$; The plaintext bits are not balanced. Let the probability of 0 be x and then the probability of 1 turns out to be $1-x$; We can calculate the probability of ciphertext bits. We find out the probability of a ciphertext bit being 1 or 0 is equal to $1/2 \cdot x + 1/2 \cdot (1-x) = 1/2$, and the ciphertext looks like a random sequence.
5) With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted C_1 obviously corrupts P_1 and P_2.
   - Are any blocks beyond P_2 affected?
     – Answer: No. For example, suppose C_1 is corrupted. The output block P_3 depends only on the input blocks C_2 and C_3.
   - Suppose that there is a bit error in the source version of P_1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?



(a) Encryption



(b) Decryption

- Answer: An error in P_1 affects C_1. But since C_1 is input to the calculation of C_2, C_2 is affected. This effect carries through indefinitely, so that all ciphertext blocks are affected. However, at the receiving end, the decryption algorithm restores the correct plaintext for blocks except the one in error. You can show this by writing out the equations for the decryption. Therefore, the error only effects the corresponding decrypted plaintext block.

6) Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? How about decryption?
   - Answer: In CBC encryption, the input block to each forward cipher operation (except the first) depends on the result of the previous forward cipher operation, so the forward cipher operations cannot be performed in parallel. In CBC decryption, however, the input blocks for the inverse cipher function (i.e., the ciphertext blocks) are immediately available, so that multiple inverse cipher operations can be performed in parallel.
7) CBC-Pad is a block cipher mode of operation used in the RC5 block cipher, but it could be used in any block cipher. CBC-Pad handles plaintext of any length. The ciphertext is longer then the plaintext by at most the size of a single block. Padding is used to assure that the plaintext input is a multiple of the block length. It is assumed that the original plaintext is an integer number of bytes. This plaintext is padded at the end by from 1 to bb bytes, where bb equals the block size in bytes. The pad bytes are all the same and set to a byte that represents the number of bytes of padding. For example, if there are 8 bytes of padding, each byte has the bit pattern 00001000. Why not allow zero bytes of padding? That is, if the original plaintext is an integer multiple of the block size, why not refrain from padding?
   - Answer: After decryption, the last byte of the last block is used to determine the amount of padding that must be stripped off. Therefore there must be at least one byte of padding.

Tutorial 3

1) Does the set of residue classes (mod 3) form a group
   - with respect to modular addition?
     - Answer: Here are the addition and multiplication tables

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

     Yes. The identity element is 0, and the inverses of 0, 1, 2 are respectively 0, 2, 1.
   - with respect to modular multiplication?
     - No. The identity element is 1, but 0 has no inverse.

2) Consider the set $S = \{a, b\}$ with addition and multiplication defined by the following tables. Is S a ring? Justify your answer.

+	a	b
a	a	b
b	b	a

×	a	b
a	a	a
b	a	b

   - Answer: S is a ring. We show it by using the axioms
     - (A1) Closure: The sum of any two elements in S is also in S.
     - (A2) Associative: S is associative under addition, by observation.
     - (A3) Identity element: a is the additive identity element for addition.
     - (A4) Inverse element: The additive inverses of a and b are a and b, respectively.
     - (A5) Commutative: S is commutative under addition, by observation.
     - (M1) Closure: The product of any two elements in S is also in S.
     - (M2) Associative: S is associative under multiplication, by observation.
     - (M3) Distributive laws: S is distributive with respect to the two operations, by observation.

3) Find the multiplicative inverse of each nonzero element in Z_5.
   - Answer:

$x \in Z_5^*$	1	2	3	4
$x^{-1}\ mod\ 5$	1	3	2	4

4) Let p be a prime number, and $2^m \not\equiv 1 \bmod p$. Please prove

$$1^m + 2^m + \cdots + (p-1)^m \equiv 0 \bmod p$$

   - Answer: Let $A = \{A_1 = 1, A_2 = 2, \cdots, A_{p-1} = p-1\}$ be one set. We can construct another set B, where $B = \{B_1 = 2 \cdot 1 \bmod p, B_2 = 2 \cdot 2 \bmod p, \cdots, B_{p-1} = 2 \cdot (p-1) \bmod p\}$. Since $\gcd(2, p) = 1$, we can see $|A| = |B|$ and two sets A and B are identical. Therefore, we have

$$\sum_{i=1}^{p-1} A_i^m = \sum_{i=1}^{p-1} B_i^m \Rightarrow \sum_{i=1}^{p-1} A_i^m \equiv \sum_{i=1}^{p-1} B_i^m \bmod p$$

     Then, we have

$$1^m + 2^m + \cdots + (p-1)^m \equiv (2 \cdot 1)^m + (2 \cdot 2)^m + \cdots + (2 \cdot (p-1))^m \bmod p$$

$$1^m + 2^m + \cdots + (p-1)^m \equiv 2^m \cdot (1^m + 2^m + \cdots + (p-1)^m) \bmod p$$

$$(2^m - 1) \cdot (1^m + 2^m + \cdots + (p-1)^m) \equiv 0 \bmod p$$

     Because $2^m \not\equiv 1 \bmod p$, we have

$$1^m + 2^m + \cdots + (p-1)^m \equiv 0 \bmod p$$

5) Let $p > 3$ be a prime number. Please prove that, for any integers a, b, we will have

$$ab^p - ba^p \equiv 0 \bmod 6p$$

- Answer:

$$ab^p - ba^p \equiv 0 \bmod 6p \Rightarrow ab^p - ab - (ba^p - ab) \equiv 0 \bmod 6p$$

We first prove $ab^p - ab \equiv 0 \bmod 6p$, and then prove $ba^p - ab \equiv 0 \bmod 6p$.
For $ab^p - ab \equiv 0 \bmod 6p$, we actually need to prove $6p|(ab^p - ab)$.
Because $b^p - b = b(b^{p-1} - 1) = b[(b^2)^{\frac{p-1}{2}} - 1] = b(b^2 - 1)[(b^2)^{\frac{p-1}{2}-1} + (b^2)^{\frac{p-1}{2}-2} \cdots + 1]$, we know

$$b(b^2 - 1)|b^p - b$$

It is easy to see

$$6|b(b^2 - 1)$$

(we can see $b(b^2 - 1)$ always has a factor 2 and a factor 3, so we have $6|b(b^2 - 1)$.) Therefore, we have

$$6|b^p - b$$

From the Fermat Little Theorem, we have

$$p|b^p - b$$

Because $\gcd(6, p) = 1$, we have

$$6p|b^p - b$$

Then, $6p|(ab^p - ab)$. Similarly, we can prove $6p|(ba^p - ab)$.
Finally, we have $ab^p - ab - (ba^p - ab) \equiv 0 \bmod 6p$, that is, $ab^p - ba^p \equiv 0 \bmod 6p$.

Tutorial 4

1) What are the principal elements of a public-key cryptosystem?
   - Answer: *Plaintext:* This is the readable message or data that is fed into the algorithm as input. *Encryption algorithm:* The encryption algorithm performs various transformations on the plaintext. *Public and private keys:* This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the encryption algorithm depend on the public or private key that is provided as input. *Ciphertext:* This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts. *Decryption algorithm:* This algorithm accepts the ciphertext and the matching key and produces the original plaintext.
2) What are the roles of the public and private key?
   - Answer: A user's private key is kept private and known only to the user. The user's public key is made available to others to use. The private key can be used to encrypt a signature that can be verified by anyone with the public key. Or the public key can be used to encrypt information that can only be decrypted by the possessor of the private key.
3) In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M?
   - Answer: $M = 5$
4) In the RSA public-key encryption scheme, each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?
   - Answer: No, it is not safe. Once Bob leaks his private key, Alice can use this to factor his modulus, N. Then Alice can crack any message that Bob sends.
     Here is one way to factor the modulus:
     Let $k = ed - 1$. Then k is congruent to $0 \bmod \phi(N)$ (where 'ϕ' is the Euler totient function). Select a random x in the multiplicative group Z_N^*. Then $x^k \equiv 1 \bmod N$, which implies that $x^{k/2}$ is a square root of $1 \bmod N$. With 50% probability, this is a nontrivial square root of N, so that
     $$\gcd(x^{k/2} - 1, N)$$
     will yield a prime factor of N.
     If $x^{k/2} = 1 \bmod N$, then try $x^{k/2}, x^{k/4}$, etc...
     This will fail if and only if $x^{k/2i} = -1 \bmod N$ for some i. If it fails, then choose a new x.
     This will factor N in expected polynomial time.
5) "I want to tell you, Holmes," Dr. Watson's voice was enthusiastic, "that your recent activities in network security have increased my interest in cryptography. And just yesterday I found a way to make one-time pad encryption practical."
   "Oh, really?" Holmes' face lost its sleepy look.
   "Yes, Holmes. The idea is quite simple. For a given one-way function F, I generate a long pseudorandom sequence of elements by applying F to some standard sequence of arguments. The cryptanalyst is assumed to know F and the general nature of the sequence, which may be as simple as $S, S+1, S+2, \cdots$, but not secret S. And due to the one-way nature of F, no one is able to extract S given $F(S+i)$ for some i, thus even if he somehow obtains a certain segment of the sequence, he will not be able to determine the rest."
   "I am afraid, Watson, that your proposal isn't without flaws and at least it needs some additional conditions to be satisfied by F. Let's consider, for instance, the RSA encryption function, that is $F(M) = M^K \bmod N$, K is secret. This function is believed to be one-way, but I wouldn't recommend its use, for example, on the sequence $M = 2, 3, 4, 5, 6, \cdots$
   'But why, Holmes?" Dr. Watson apparently didn't understand. "Why do you think that the resulting sequence $2^K \bmod N$, $3^K \bmod N$, $4^K \bmod N$, $\cdots$ is not appropriate for one-time pad encryption if K is kept secret?"
   "Because it is at least partially predictable, dear Watson, even if K is kept secret. You have said that the cryptanalyst is assumed to know F and the general nature of the sequence. Now let's assume that he will obtain somehow a short segment of the output sequence. In crypto circles, this assumption is generally considered to be a viable one. And for this output sequence, knowledge of just the first two elements will allow him to predict quite a lot of the next elements of the sequence, even if not all of them, thus this sequence can't be considered to be cryptographically strong. And with the knowledge of a longer segment he could predict even more of the next elements of the sequence. Look, knowing the general nature of the sequence and its first two elements $2^K \bmod N$ and $3^K \bmod N$, you can easily compute its following elements."
   Show how this can be done.
   - Answer: 3rd element, because it equals to the 1st squared, 5th element, because it equals to the product of 1st and 2nd, 7th element, because it equals to the cube of 1st, etc.

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.

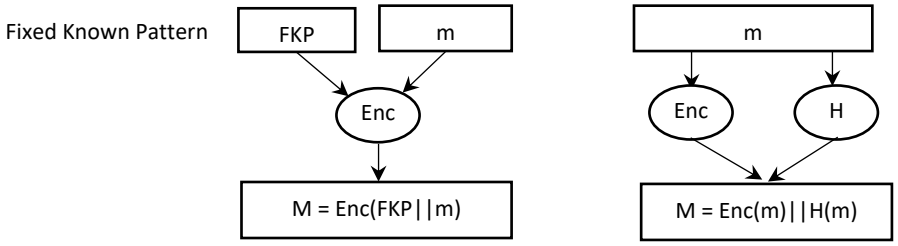
Question 2.

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.

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