CSE 461 Theory Assignment

2 MARK QUESTIONS

1) Why One Time Pads (OTP) are called information-theoretically secure?

Answer

The encrypted message (i.e., the ciphertext) in One Time Pad provides no information about the original message to a cryptanalyst.

That is why OTPs are called information-theoretically secure.

2) While AES encryption, which of the four round steps implements p-box?

Answer

In AES encryption, each round has four steps as mentioned below –

- Substitute Bytes()
- Shift Rows()
- Mix Columns()
- Add Round Key()

Among these, shiftRows and shiftColumns step implements P-Box combinedly.

3) How does a known-plaintext attack differ from a ciphertext-only attack?

Answer

In known-plaintext attack, the cryptanalyst has access to one or more plaintext-ciphertext pairs, such that each plaintext was encrypted using the same key. His or her goal in this case is to determine the key.

But in ciphertext-only attack, he cryptanalyst has access to the ciphertext of one or more messages, all of which were encrypted using the same key, K. His or her goal is to determine the plaintext for one or more of these ciphertexts or, to discover K.

4) Why AES is considered more secure than DES?

Answer

DES = Data Encryption Standard

AES = Advanced Encryption Standard

DES is insecure due to the relatively short 56 bits key size. Around 50 hours of brute-forcing is able to crack the message.

AES allows to choose the option for various key lengths like 128-bit, 192-bit or 256-bit key,

making it exponentially stronger than the 56-bit key of DES.

5) Define Key exchange protocol.

Answer

A key exchange protocol is a cryptographic approach to establishing a shared secret key by communicating solely over an insecure channel, without any previous private communication.

Diffie-Hellman is such a protocol.

6) Explain collision resistance property of a cryptographic hash function.

Answer

It should be infeasible to find any pair of distinct inputs

m1, m2 such that H(m1) = H(m2).

7) Explain the role of S-box and P-box in AES.

Answer

AES takes a block of the plaintext and the key as inputs, and applies several alternating rounds or layers of S-boxes and P-boxes to produce the ciphertext block.

An S-box substitutes a small block of bits (the input of the S-box) by another block of bits (the output of the S-box).

A P-box takes the outputs of all the S-boxes of one round, permutes the bits, and feeds them into the S-boxes of the next round.

8) Explain shannon's confusion property.

Answer

Shannon's confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.

9) Using shift key 15, decrypt the following Caesar cipher : **DPNFCTEJLDDTRYXPYE**

Answer

In Caeser cipher, every character is replaced with the character K slots to the right.

K is the shift key value.

Subtracting 15 from the encrypted letters gives-

D-> S

P-> E etc.

In this way, the whole encrypted message is decrypted as such -

SECURITYASSIGNMENT

10) For 192 bit key size, how many round keys are needed during Encryption?

Answer

For 192 bit key size, AES goes through 12 rounds. So, $N_r = 12$.

We know -

Number of round keys = $N_r + 1$

$= 12 + 1$

$= 13$

So, taking into consideration the initial round, a total of 13 round keys will be generated.

11) What is pretexting?

Answer

Pretexting is a social engineering approach which focuses on creating a story that convinces an

administrator or operator into revealing secret

information.

12) State some candidates for Biometric IDs.

Answer

Biometric refers to any measure used to uniquely identify a person based on biological or physiological traits.

Some of the Biometric ID candidates are-

Fingerprints

Retinal/iris scans

DNA

Blue-ink signature

Voice recognition

Face recognition

Gait recognition

13) Explain some shoulder surfing techniques used in eavesdropping.

Answer

Following are some of the direct observation techniques used in eavesdropping which are commonly referred to as shoulder surfing -

– Using social engineering to allow the attacker to read information over

the victim's shoulder

– Installing small cameras to capture the information as it is being read

– Using binoculars to view a victim's monitor through an open window.

14) What is RFID?

Answer

Radio frequency identification, or RFID, is a rapidly emerging technology that relies on small transponders to transmit identification information via radio waves.

15) What is masquerading?

Answer

Masquerading is the fabrication of information that is purported to be from someone who is not actually the author.

5 MARK QUESTIONS

1) Given e=13, n=77 find out private and public key according to the principle of RSA algorithm.

Answer

For n=77, p and q value should be 7 and 11 respectively.

And e=13 given.

$\Phi(n) = (p-1) * (q-1) = (7-1) * (11-1) = 6 * 10 = 60$

Finding d:

$e * d \bmod \Phi(n) = 1$

$d = ((\Phi(n) * i) + 1) / e$

now we go on incrementing i value until an integer for d is found –

$d = (1*60 + 1) / 13 = 4.69$ (∵ i = 1)

$d = (2*60 + 1) / 13 = 9.30$(∵ i = 2)

$d = (3*60 + 1) / 13 = 13.92$ (∵ i = 3)

$d = (4*60 + 1) / 13 = 18.53$(∵ i = 4)

$d = (5*60 + 1) / 13 = 23.15$ (∵ i = 5)

$d = (6*60 + 1) / 13 = 27.76$ (∵ i = 6)

$d = (7*60 + 1) / 13 = 32.38$ (∵ i = 7)

$d = (8*60 + 1) / 13 = 37$ (∵ i = 8)

so d value is 37

Hence, public key {13, 77} and private key {37, 77}

2) Explain the major properties of Digital Signature.

Answer

A digital signature is a cryptographic technique used to provide authentication, integrity, and non-repudiation in electronic communication or digital data transactions.

- Data origin authentication: Assurance of who originated (signed) a message or file. Establishing the certainty of the sender's identity through the application of a digital signature, ensuring the authentication of the message or file origin.
- Data integrity: Assurance that received content is the same as that originally signed.
- Non-repudiation: Offering robust evidence of the unique initiation of digital data, creating formidable barriers for any party attempting to digitally sign information and subsequently deny their involvement in the process. Strong evidence of unique origination, making it hard for a party to digitally sign data and later successfully deny having done so.

.....

3) How the Elgamal Cryptosystem makes the communication secured?

Answer

The ElGamal Cryptosystem secures communication through public-key cryptography that uses randomizations. Users generate a public key (p, g, y) for sharing and a private key for confidentiality.

y = g^x mod p

The security of this scheme is based on the fact that, without knowing x, it would be very difficult for an eavesdropper to decrypt the ciphertext, (a, b)

When sending a message, the sender encrypts a randomly generated symmetric key with the recipient's public key. The recipient uses their private key to decrypt the symmetric key, ensuring secure message transmission. ElGamal's strength lies in the discrete logarithm problem's complexity. Regular key management is vital, and the system provides non-repudiation, making it computationally challenging for unauthorized entities to decrypt messages or forge signatures without the private key.

.....

4) What type of practical problems do we face while working with OTP?

Answer

One-Time Pads (OTPs) are a type of symmetric key encryption where a unique key is used only once for a single communication session and randomly generated.

But working with this may yield some security issues.

• The Key has to be as long as message and also has to be secret. But the key itself reveals the message size.

• It gets extremely difficult to generate truly random key. True random number generators exist but are typically slower and more specialized which may not be cost efficient.

• OTP has a very limited practical usage. A common use of the one-time pad in quantum cryptography is being used in association with Quantum Key Distribution (QKD).

• Vulnerable to reused key attacks. Keys must never be used twice! But as the keys are randomly generated, it would cause repetation if true random keys are not generated.

.....

5) Write the differences between ECB and CTR mode of block cipher operation.

Answer

ECB	CTR
Each encryption block operation is independent of adjacent blocks	Each encryption block operation is partially dependent of adjacent blocks
If a given key k is used to encrypt several identical plaintext blocks mi then identical ciphertext blocks ci result	If a given key k is used to encrypt several identical plaintext blocks mi then different ciphertext blocks ci result

.....

6) What are the major basic functions the AES process repeats in each round? Mention the functions for both encryption and decryption process.

Answer

AES basically repeats 4 major functions per round (mostly) to encrypt data.

For 128 bits key size, AES performs 10 rounds and repleats these 4 major functions in each round. Though there are some difference noticed in last round for both cases of encryption and decryption.

During encryption :

The functions are:

➢ Substitute Bytes()
➢ Shift Rows()
➢ Mix Columns()
➢ Add Round Key()

These 4 functions continue to perform for each round except the last one. The last round does't perform the Mix Columns() step, rather it directly adds the round key to finish up the operation.

So, for last round,

➢ Substitute Bytes()
➢ Shift Rows()
➢ Add Round Key()

During decryption :

The functions are:

➢ Inverse Mix Columns()
➢ Add Round Key()
➢ Inverse Substitute Bytes()
➢ Inverse Shift Rows()

Like the encryption process, the decryption process also skips the Inverse Mix Columns() function for the last round.

The last round of decryption performs the following steps:

➢ Add Round Key()
➢ Inverse Substitute Bytes()
➢ Inverse Shift Rows()

.....

7) "Cryptography is not the solution to security" - explain the statement.

Answer

Cryptography alone isn't a comprehensive security solution. Effective security requires a multi-layered approach encompassing policies, user education, and system design.

Using cryptography needs to get perfect implementation with proper decisions. While working with Cryptography, it is difficult to get right -

• Choice of encryption algorithms

• Choice of parameters

• Implementation

• Hard to detect errors : vulnerability can only be recognized after exploitation

Therefore, Cryptography serves as a vital component but must complement other measures for robust protection.

.....

8) Differentiate between AES & DES.

Answer

The major differences between AES and DES :

	DES	AES
Developed	1977	2000
Key Length	56 bits	128, 192, or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128 bits
Security	Proven inadequate	Considered secure

.....

9) Perform the Vigenère cipher operation with the provided ciphertext and the key to decrypt the ciphertext. Explain the Procedure.

Encrypted Ciphertext : ZYDEQOSJFV

Key : SUSTCSE

Answer

First the Key size need to be equalled with the size of ciphertext. This process would need the repeatation of the key.

The ciphertext has 10 characters and Key has only 7. So considering proper repeatation of the key to yield the final key, we get

key = SUSTCSESUS

Now the core Vigenère cipher decryption process works with the produced key and provided ciphertext to extract the original message.

We need to convert the characters into numeric values and them sum

.....

10) How does barcodes perform authentication?

Answer

First-generation barcodes represent data as a series of variable-width, vertical lines of ink, which is essentially a one-dimensional encoding scheme.

Recent barcodes are rendered as two-dimensional patterns using dots, squares, or other symbols

that can be read by specialized optical scanners, which translate a specific type of barcode into its encoded information.

The airline industry incorporates barcodes into boarding passes. For authentication they perform the followings -

- In most cases, the barcode is encoded with an internal unique identifier that allows airport security to look up the corresponding passenger's record with that airline.
- Staff then verifies that the boarding pass was in fact purchased in that person's name (using the airline's database), and that the person can provide photo identification.
- In most other applications, however, barcodes provide convenience but not security. Since barcodes are simply images, they are extremely easy to duplicate.

10 MARK QUESTIONS

1)

Alice wants to send a secret message to Bob using the Caesar cipher. She chooses a shift value of 3. Her original message is:

"HELLO"

a) Encode the message using the Caesar cipher.

b) Decode the message received by Bob assuming he knows the shift value.

Charlie and David want to communicate securely using the Vigenère cipher. They agree on the keyword "CODE". Charlie's message is:

"MEETMEATTEN"

c) Encrypt the message using the Vigenère cipher with the keyword "CODE".

d) Decrypt the message received by David assuming he knows the keyword.

Answer

a) Encoding:

Original message: "HELLO"

Shift value: 3

To encode each letter, we shift it by 3 positions in the alphabet:

H + 3 = K

E + 3 = H

L + 3 = O

L + 3 = O

O + 3 = R

So, "HELLO" becomes "KHOOR".

b) Decoding:

Encoded message received by Bob: "KHOOR"

Since Bob knows the shift value is 3, he reverses the process:

K - 3 = H

H - 3 = E

O - 3 = L

O - 3 = L

R - 3 = O

So, "KHOOR" decodes back to "HELLO".

c) Encryption:

Original message: "MEETMEATTEN"

Keyword: "CODE"

To encrypt using the Vigenère cipher, we repeat the keyword to match the length of the message:

Message: MEETMEATTEN

Keyword: CODECODECOD

Then, we shift each letter of the message by the corresponding letter of the keyword:

M + C = O

E + O = L

E + D = H

T + E = X

M + C = O

E + O = L

A + D = G

T + C = W

T + O = D

E + D = H

N + C = K

So, "MEETMEATTEN" encrypted with the keyword "CODE" becomes "OLHCZGQWKXDM".

d) Decryption:

Encrypted message received by David: "OLHCZGQWKXDM"

Using the keyword "CODE" again:

O - C = M

L - O = E

H - D = E

C - E = T

Z - C = M

G - O = E

Q - D = A

W - C = T

K - O = T

X - D = E

D - C = N

M - O = E

So, "OLHCZGQWKXDM" decrypted with the keyword "CODE" becomes "MEETMEATTEN".

.....

2) Using the Hill cipher with the given key matrix

| G Y B |

| N Q K |

| U R P |

encrypt the plaintext "CAT". Also decrypt the cypher text.

Answer

To encrypt "CAT" using the Hill cipher, we first need to convert the letters to their corresponding numerical values (A=0, B=1, ..., Z=25):

C => 2

A => 0

T => 19

Next, we represent these numerical values as a column vector:

| 2 |

| 0 |

| 19 |

Now, we multiply the key matrix by the plaintext vector modulo 26:

$C=(K\times P) \% 26$

K=
| 6 24 1 |
| 13 16 10 |
| 20 17 15 |

C= | 6 24 1 | | 2 |

| 13 16 10 | * | 0 | %26

| 20 17 15 | | 19 |

= | 5 |

| 12 |

| 1 |

Now, we convert these numerical values back to letters:

5 => F

12 => M

1 => B

So, the encrypted ciphertext for the plaintext "CAT" using the Hill cipher with the given key is "FMB".

To decrypt the ciphertext "FMB" using the Hill cipher, we need to use the inverse of the key matrix. Let's calculate the inverse of the given key matrix K:

K^{-1}=
| 8 5 10 |
| 21 8 21 |
| 21 12 8 |

$P = K^{-1} \times C \bmod 26$

P= | 8 5 10 | | 5 |

| 21 8 21 | * | 12 | %26

| 21 12 8 | | 1 |

= | 210 |

| 442 | %26

| 305 |

= | 2 |

| 0 |

| 19 |

Now, we convert these numerical values back to letters:

2 => C

0 => A

19 => T

So, the decrypted plaintext for the ciphertext "FMB" using the Hill cipher with the given key is "CAT".

.....

3) Decribe any 2 Modes of Operation of Block Ciphers with appropriate diagram.

Answer

ECB:

ECB (Electronic Codebook) is a mode of operation for block ciphers in cryptography. It is one of the simplest modes and involves encrypting each block of plaintext independently with the same key. Each block of plaintext is treated as a separate entity and encrypted into a corresponding block of ciphertext.

Here's how ECB works:

Divide into Blocks: The plaintext message is divided into fixed-size blocks, typically of 64 or 128 bits.

Encryption: Each block of plaintext is encrypted independently using the same encryption key and the chosen block cipher algorithm. The same key is used for every block.

Output: The resulting ciphertext blocks are concatenated to form the complete ciphertext.

Key characteristics of ECB mode:

Deterministic: The same plaintext block always encrypts to the same ciphertext block with the same key. This makes ECB deterministic and lacks diffusion (the spreading of input data over the entire block).

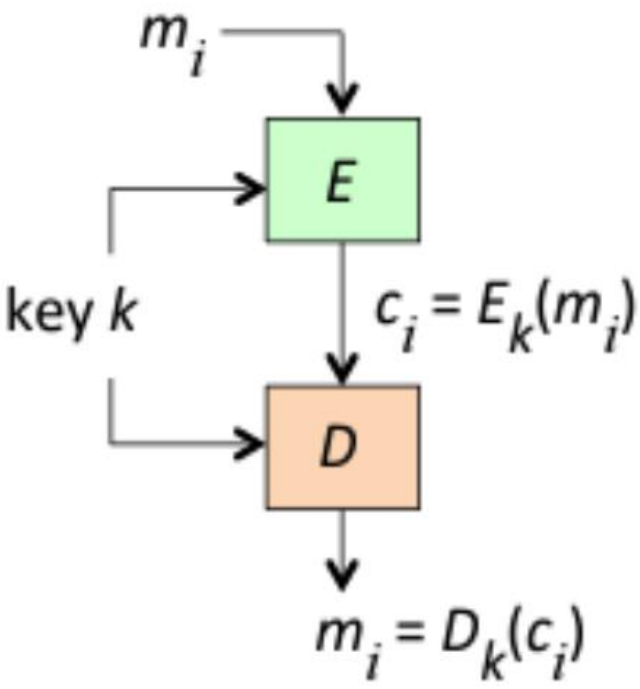
Parallelization: ECB allows for easy parallelization because each block can be encrypted independently. This property can be advantageous in certain situations but also comes with security implications.

However, ECB has several weaknesses:

Patterns: Identical plaintext blocks result in identical ciphertext blocks, which can leak information about the plaintext. This means that patterns in the plaintext are preserved in the ciphertext, which can be exploited by attackers.

Lack of security: Due to its deterministic nature and vulnerability to pattern recognition attacks, ECB is considered insecure for many applications, especially when encrypting large amounts of data.

Because of these weaknesses, ECB is generally not recommended for secure communication or data storage, and other block cipher modes such as CBC (Cipher Block Chaining) or GCM (Galois/Counter Mode) are preferred for most cryptographic applications.



CBC:

CBC (Cipher Block Chaining) is a mode of operation for block ciphers in cryptography. It enhances the security of encryption by introducing feedback from the previous ciphertext block into the encryption of the current block. CBC mode operates on fixed-size blocks of plaintext, typically 64 or 128 bits.

Here's how CBC works:

Initialization Vector (IV): CBC requires an initialization vector, which is a fixed-size random value. This IV is XORed with the first block of plaintext before encryption.

XOR Operation: Each plaintext block (except the first one) is XORed with the ciphertext block preceding it before encryption. This creates a feedback mechanism where each ciphertext block depends on the previous ciphertext block.

Encryption: After the XOR operation, each resulting block of plaintext is encrypted using the chosen block cipher algorithm with the encryption key.

Output: The resulting ciphertext blocks are concatenated to form the complete ciphertext.

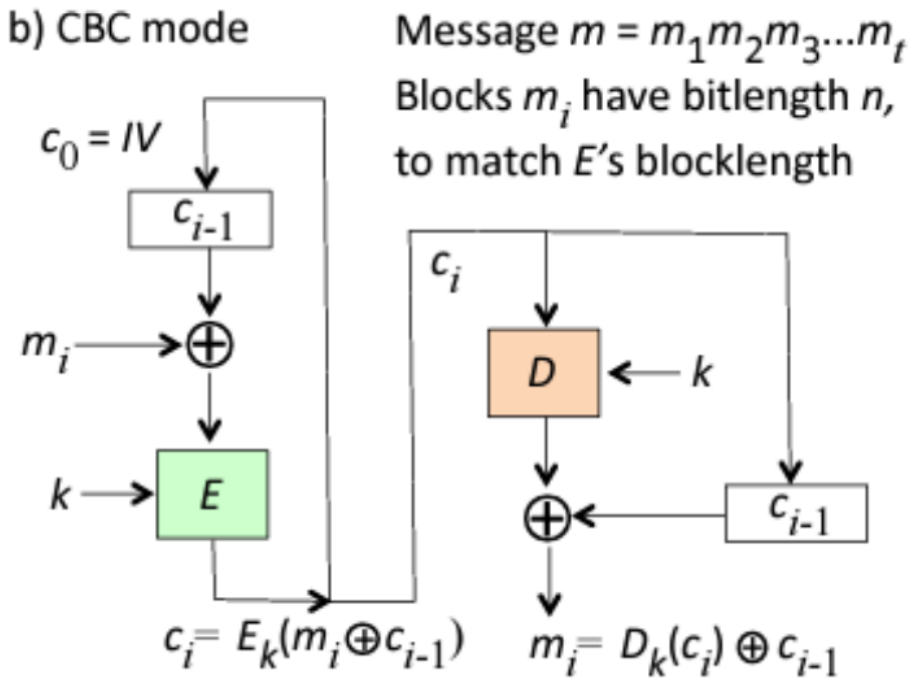
Key characteristics of CBC mode:

Initialization Vector (IV): The IV ensures that even if the same plaintext is encrypted multiple times with the same key, the resulting ciphertext will be different. The IV should be unique for each encryption operation.

Diffusion: CBC mode provides diffusion, meaning that changes in one part of the plaintext result in changes throughout the ciphertext. This makes it resistant to pattern recognition attacks.

Decryption: To decrypt the ciphertext, each block is decrypted using the same key and then XORed with the previous ciphertext block. The IV is XORed with the first block of decrypted plaintext.

CBC mode provides a higher level of security compared to ECB mode because it introduces feedback and diffusion. However, CBC mode requires more computation and cannot be parallelized as easily as ECB mode due to the dependency between blocks. Additionally, care must be taken to securely manage and transmit the IV to maintain the security of the encryption.



4) What potential threats can compromise the RSA cryptosystem? Provide an example of an attack and discuss preventive measures against it.

Answer

Eavesdropping can compromise the RSA cryptosystem to a great extent. This may hamper digital signature scheme.

Following is an example of such an attack along with appropriate measures to prevent those –

Let's take a scenario where a sender names Alice is transmitting data to Bob, who is the receiver. While the transmission takes place, an eavesdropper interferes and modifies the data and then retransmits the data to Bob. Bob uses hashing to detect if the encrypted messages are forged or not.

- ALICE (sender)
  - Creates two messages M1, M2 (in a gap of seconds)
  - Generates Hashes
    - H1 = H(M1)
    - H2 = H(M2)
  - Generates signatures
    - $S1 = H1^d \bmod n$
    - $S2 = H2^d \bmod n$
  - Transmits these pairs (M1,S1), (M2,S2) to Bob through communication channel

- EVE (eavesdropper)
  - Receives the pairs (M1,S1), (M2,S2)
  - Creates new message
    - M = M1 * M2
  - Generates new signature
    - S= S1 * S2
  - Retransmits to (M,S) to Bob

❖ BOB (receiver)

- Receives (M,S)
- Applying hash on M
  - H` = H(M) = H (M1 * M2)
- Applying public key {e,n} on signature

  - $H`` = S^e \bmod n$
    $= \{S1 * S2\}^e \bmod n$
    $= \{(H1^d \bmod n)*(H2^d \bmod n)\}^e \bmod n$
    $= \{(H1^{de} \bmod n)*(H2^{de} \bmod n)\} \bmod n$
    $= \{(H1^{de \bmod \Phi(n)} \bmod n)*(H2^{de \bmod \Phi(n)} \bmod n)\} \bmod n$
    $= \{(H1^1 \bmod n)*(H2^1 \bmod n)\} \bmod n$
    $= \{ H1*(H2)\} \bmod n$
    $= H1*H2$
    $= H(M1) * H(M2)$

Since H(M1) * H(M2) ≠ H (M1 * M2), forgery detected in the transmitted data.

This is how hashing helps in detecting forgery in RSA digital signature scheme.

.....

5) What kind of security measures does the ATM technology take and what kind of attacks can be performed on it? Explain with details.

Answer

An automatic teller machine (ATM) is any device that allows customers of financial institutions to complete withdrawal and deposit transactions without human assistance.

Typically, customers insert a magnetic stripe credit or debit card, enter a PIN, and then deposit or withdraw cash from their account.

The ATM has an internal cryptographic processor that encrypts the entered PIN and compares it to an encrypted PIN stored on the card or in a remote database. To ensure the confidentiality of customer transactions, each ATM has a cryptographic processor that encrypts all incoming and outgoing information, starting the moment a customer enters their PIN. The current industry standard for ATM transactions is the Triple DES

(3DES) cryptosystem, a legacy symmetric cryptosystem with up to 112 bits of security. The 3DES secret keys installed on an ATM are either loaded on-site by technicians or downloaded remotely from the ATM vendor.

Attackers can possibly attack the ATM system of an individual or a group to have illegal access to it. They can perform the attack in various ways.

• Lebanese loop: A perpetrator inserts this sleeve into the card slot of an ATM. When a customer attempts to make a transaction and inserts their credit card, it sits in the sleeve, out of sight from the customer, who thinks that the machine has malfunctioned. After the customer leaves, the perpetrator can then remove the sleeve with the victim's card.

• Skimmer: a device that reads and stores magnetic stripe information when a card is swiped. An attacker can install a skimmer over the card slot of an ATM and store customers' credit information without their knowledge. Later, this information can be retrieved and used to make duplicates of the original cards.

• Fake ATMs: capture both credit/debit cards and PINs at the same time.

.....

6) In RSA, two prime numbers are picked in the setup phase, p = 61, q = 53 and e = 17.

(a) Find the private key d.

(b) Let's assume, message M = 13. Find the cipher C of the message M. In this case, use the value n = 143 and e = 13

Answer

(a) The given prime numbers are $p = 61$ and $q = 53$

Then, $n = 53 \times 61 = 3233$

Then we need to compute,

$$\Phi(n) = \Phi(p) \times \Phi(q)$$

$$= \Phi(53) \times \Phi(61)$$

$$= 52 \times 60$$

$$= 3120$$

We are given the value $e = 17$

Now,

$$e\,d = 1 \bmod \Phi(n)$$

$$\Rightarrow \quad d = e^{-1} \bmod \Phi(n)$$

$$\Rightarrow \quad d = 2753$$

Private key $d = 2753$

$(d,e) = (2753, 3233)$

(b) The given message is $M = 13$

We know, Encryption , $C = P^e \bmod n$

Now we need to calculate the cipher C of the message M.

$$C = P^e \bmod n$$

$$= 13^{13} \bmod 143$$

$$= \{(13^8 \bmod 143)\ (13^4 \bmod 143)\ (13 \bmod 143)\} \bmod 143$$

$$= (91 \times 104 \times 13) \bmod 143 = 52$$

$$C = 52$$

The encoded ciphertext of the given message C = 52.

.....

7) What is the minimum number of people required for there to be a 60% probability of at least two individuals sharing the same birthday?

Answer

We know,

$P(k) \approx 1 - e^{-2m/2^*k}$

To find the value of k when P(k) is 60%, we need to solve the equation:

$0.6 = 1 - e^{-k^*k/2^*m}$

$\Rightarrow e^{-k^*k/2^*m} = 0.4$

$\Rightarrow \ln(e^{-k^*k/2^*m}) = \ln(0.4)$

=> −k*k/2*m =ln(0.4)
=> k*k=−2*m*ln(0.4)
=> k*k=−2*m*ln(0.4)
=> k*k=−2*365*ln(0.4)
=>k= 27.52

So, when P(k) is 60%, approximately 27.52 people are needed in the group for there to be a 60% chance that at least two of them share the same birthday. Since you can't have a fraction of a person, you would round up to 28 people.

.....

8) Given a scenario, Sherlock and Watson are sharing a key under the Diffie-Hellman protocol to transmitting a secret information. Both of them picked up a prime number, p = 701 and a primitive root, g= 21.

Sherlock and Watson selected S=17 and W=23 for sharing keys.

But their arch rival Jim is eavesdropping on the communication channel they are using. Jim wants to launch a MITM attack for which he chooses s=13 and w=19 for attacking Sherlock and Watson respectively.

i) Determine the key is shared between Sherlock and Watson or not.
ii) Does the shared key between Jim and Sherlock differ from that between Jim and Watson? Explain with reason.

Answer:

(i)

For simplicity –

Let,

S=x=17, W=y=23

Given –

P=701 and g=21

Sherlock will compute,

$X = g^x \bmod p$

$= 21^{17} \bmod 701$

$= 73$

Similarly Watson will compute,

$Y = g^y \bmod p$

$= 21^{23} \bmod 701$

$= 11$

Sherlock will compute secret key as,

$K1 = Y^x \bmod p$

$= 11^{17} \bmod 701$

$= 662$

Watson will compute secret key as,

$K2 = X^y \bmod p$

$= 73^{23} \bmod 701$

$= 662$

Hence the key is shared between Sherlock and Watson.

(ii)

For simplicity –

Let,

s=13 and t=19

Since the transmission is eavesdropped, Sherlock and Jim would compute the secret key as –

$K1 = g^{xs} \bmod p$

$= 21^{17*13} \bmod 701$

$= 21^{221} \bmod 701$

= 489

And Watson and Jim would compute the secret key as –

$K2 = g^{yt} \bmod p$

$= 21^{23*19} \bmod 701$

$= 21^{437} \bmod 701$

= 188

So, as we can see here, the shared key between Jim and Sherlock differs from that between Jim and Watson due to Jim acting as an eavesdropper and modifying the data.

.....END.....