CSE470 Soruları

2016 Vize

1- a) Kriptolamayı tanımlayarak mutlak ve hesaplamaya bağlı güvenlik ile Kriptografik algoritmalarında ayrık logaritma problemi nedir? Kısaca açıklayınız?

Cevap:

Encrypting is the conversion of text or text into a meaningless form, depending on a rule, to prevent it from being read by others.

The discrete logarithm is defined over finite cyclic groups and is the inverse of x^a=b (mod p) on a finite circular group Z_p* (p is a prime number). The Discrete logarithm problem used in the design of digital signing algorithms is the difficulty of finding the value that satisfies this equation. Because there is not a single value for the number a and when very large numbers are used, this set expands even more.

1- b) [a mod n – b mod n] mod n = (a - b) mod n eşitsizliğini ispatlayınız?

Cevap:

Lets say

a mod n = a + n.x

b mod n = b + n.y

[a mod n - b mod n] mod n = [(a + n.x) - (b + n.y)] mod n

= [(a-b) + n.(x-y)] mod n

= [(a-b) mod n] - [n.(x-y) mod n]

since n.(x-y) mod n = 0

= [(a-b) mod n] - 0

= (a-b) mod n

---

2) Yerine koyma ve yer değiştirme tabanlı şifreleme nedir? Sakıncaları nelerdir ve çözümleri nelerdir açıklayınız?

Cevap:

Substitution cipher vs transposition cipher

A substitution cipher is a method of encrypting in which units of plaintext are replaced with the ciphertext

Disadvantage : the last letters of the alphabet (which are mostly low frequency) tend to stay at the end

Solutions :

Polyalphabetic Ciphers:improve security using multiple cipher alphabets

Vigenere Cipher :simplest polyalphabetic substitution cipher, has multiple-26 ceasar ciphers

A transposition cipher is a method of encryption which scrambles the positions of characters (transposition) without changing the characters themselves.

Disadvantage : Since transposition does not affect the frequency of individual symbols, simple transposition can be easily detected by the cryptanalyst by doing a frequency count

Solutions :

Rail Fence Cipher : write message letters out diagonally over a number of rows then read off cipher row by row
Row Transposition Cipher : write letters of message out in rows over a specified number of columns
then reorder columns according to some key before reading off rows

---

3) Güçlü şifreleme algoritmaları için gerekli yöntemler nelerdir? Şifreleme yöntemlerini açıklayınız ve brute force saldırılarına zorlanmalarının sebeplerini belirtiniz?
Cevap:
Symmetric Encryption
aka private-key cryptography, sender and receiver have access to the same key. Recipient needs to have the key before the message is decrypted

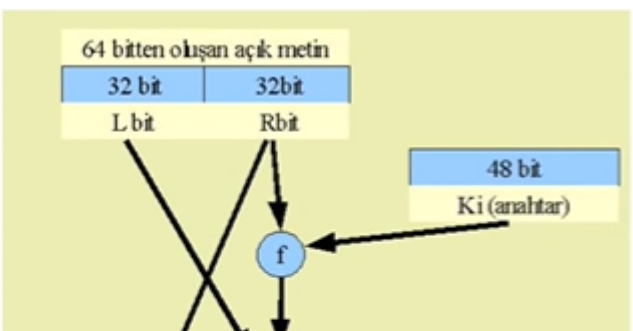
Asymmetric Encryption
aka public-key cryptography, there are two keys for encryption process, a public and a private key. User employs one key for encryption and the other for decryption
Public key is available to everyone, private key remains with the intended recipients only who need it to decipher messages.

the private and public keys have a mathematical relation between them, and asymmetric ciphers are based on problems that are computationally hard to solve

Hashing
Generates a unique structure of fixed length for a message.Each message has its unique hash, making minor changes to the info easily trackable. Data encrypted with hashing cannot be deciphered into its original form.

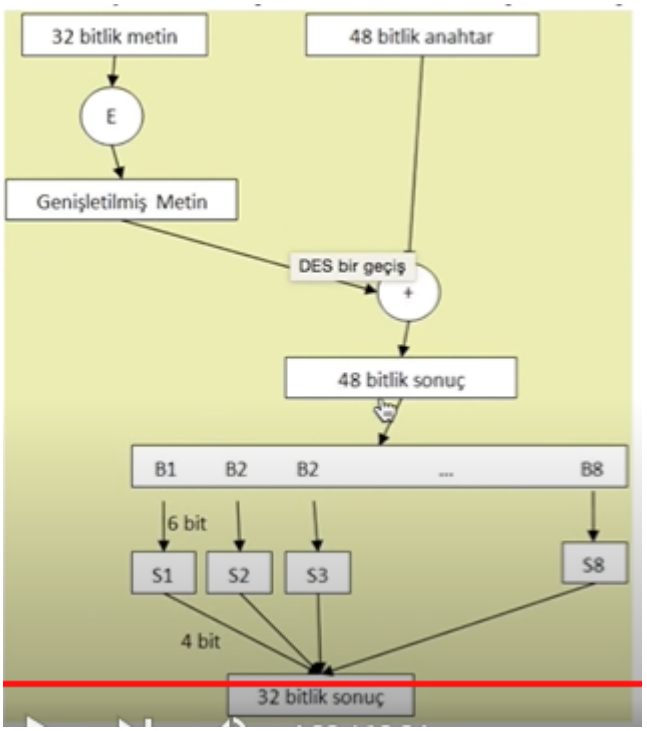
---

4 – a) DES yönteminin bir turunda yapılan işlemlerini yazınız?
Cevap:
a) DES one round

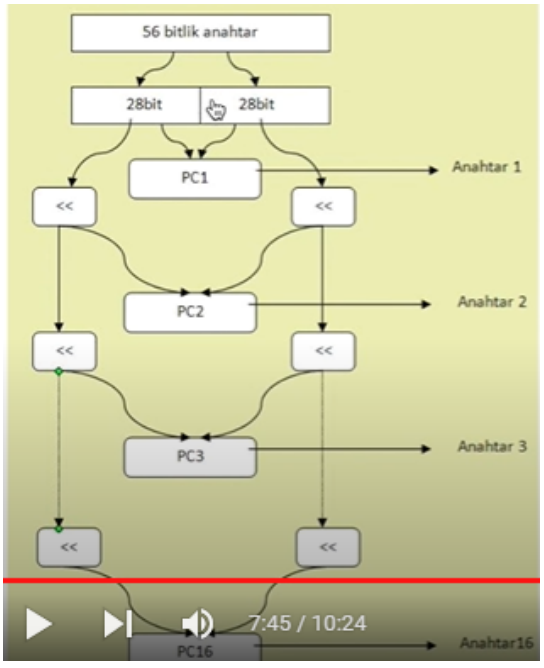


message is 64 bit, divided into two halves 32 bit length
there is a key with 64 bit length. R bit goes directly to the left of the result ciphertext. L bit goes to the xor with the result of the function Function inputs are Rbit of the plaintext and the 48 bit key. Then result of the xor becomes Rbit of the result ciphertext. These operations are repeated 16 times for a block.

64 bit key => 48 bit key + 8 bit parity bit + 8 bit each repeat of round we use different key



Rbit of the plaintext becomes 48 bit by using expansion table. Some values 1..32 are repeated. some bits are transformed into 2 bits. Then this expanded text goes xor with 48 bit key. Then result is divided into 8 Blocks with 6 bit length. These blocks goes to S-boxes(substitution boxes). Result of the These S-boxes are 4 bits. It works like inverse of expansion table. So we have 8 blocks and 4 bits for each block, we have 32 bit result. This is the output of the f function.

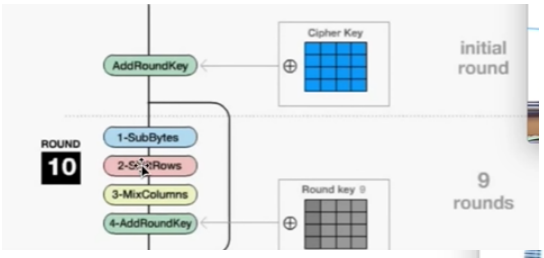


Key Generator
56 bit key divided into two halves 28 bit length
0..3 4...51 52...55
then the one that starts with 4..51 becomes the key1 then the halves shifted left one time. Then these operations repeated for 16 times. Then 16 different key is generated for 16 rounds.

---

4 – b) AES yöntemi için (a da) yapılan işlemleri yazınız?

Cevap:

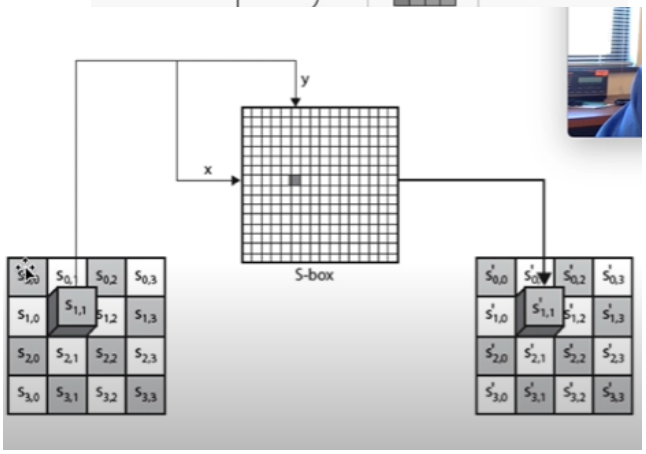


Block length = 128

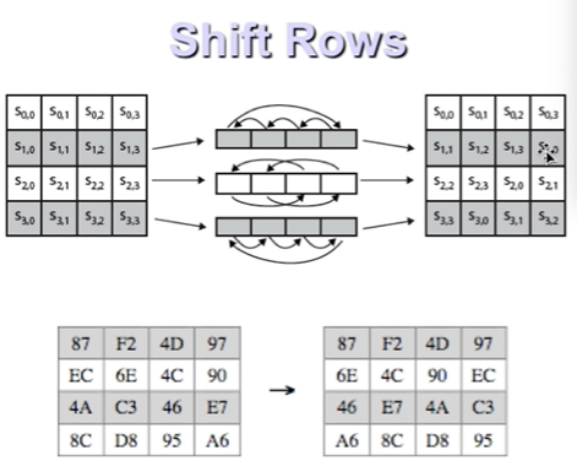
Support for key length of 128,192,256

Substitute Bytes

We have 16 S boxes, there are 8 bits in each box, so we have 128 bit message.



Think of 8 bit message 4 bit + 4 bit. Then each 4 bit can represent 16 numbers. Then we have 16x16 table so, if we have 1010 as binary 4 bit, then we get 10th entry of the table. so let's say that 8 bit number is 1010 1101 so we will get 10 and 13, which are x and y, then take this number (1010 1101) then put it to the 10th row and 13 column in the table. (Each entry in the table is 8 bit)



87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

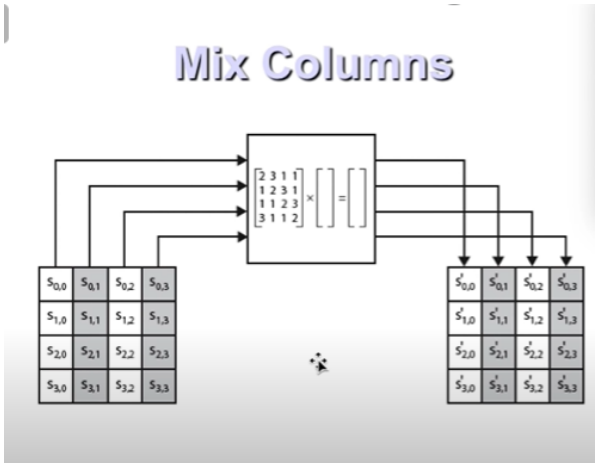
Shift rows

at first row, no shift

at second row, shift to the left once

at third row, shift twice to the left

at fourth row, shift three times to the left



Mix Columns

We have a matrix, then we take each column and multiply with the matrix, then we write result to the same place

Add round key
Message is 128 bit, key is 128 bit, we xor them and get the result, we apply these operations 10 time

---

5 – a) Mac ve Hash fonksiyonu ne demektir? Collision resistance nedir?
Cevap:
It is a message integrity and authenticity method which combines hashing and MAC(message authentication code). It uses two keys to generate authentication code and appends it to the message. [m | h(k2 | (h(k1 | m))]
Two messages can have the same hash value. This is called a collision. Collision resistance is the capability of the hash functions to evenly distribute hashes to avoid collisions.

---

5 – b) D – H (Diffie - Hellman) yönteminin çalışmasını yazınız?
Cevap:
It is used for changing keys in cryptography. Let's think of a scenario where Alice and Bob wish to swap keys

Select two prime numbers, a = 3 and q = 17; these are public to anyone
Alice's private key is p1 = 15
Bob's private key is p2 = 13

Alice sends the number a^p1 mod q = 3^15 mod 17 = 6 to Bob
Bob sends the number a^p1 mod q = 3^13 mod 17 = 12 to Alice

Alice generates the new key with 12^15 mod 17 = 10
Bob generates the new key with 6^13 mod 17 = 10

Since only Alice and Bob know their private key, nobody else can find the new generated key other than them.

2017 Final

1- a) Simetrik ve Asimetrik şifrelemeyi tanımlayınız ve farklarını belirtiniz.
Mutlak güvenlik ve hesaplamaya bağlı güvenlik nedir? Kısaca açıklayınız?
Cevap:

Symmetric Key encryption: In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.

Asymmetric Key Encryption: Asymmetric Key Encryption is based on public and private key encryption techniques. It uses two different key to encrypt and decrypt the message. It is more secure than the symmetric key encryption technique but is much slower.

Symmetric Key encryption vs Asymmetric Key Encryption:

- Symmetric-key encryption only requires a single key for both encryption and decryption. Asymmetric Key Encryption requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
- Symmetric-key encryption only provides confidentiality. Asymmetric Key Encryption provides confidentiality, authenticity, and non-repudiation.
- While the encryption process is very fast in symmetric key encryption, the encryption process is slow in asymmetric encryption.
- In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption. In asymmetric key encryption, resource utilization is high.
- In symmetric key encryption, security is less as only one key is used for both encryption and decryption purpose. Asymmetric key encryption is more secure as two keys are used here- one for encryption and the other for decryption.

Unconditional Security
No matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext.

Computational Security
given limited computing resources (e.g. time needed for calculations is greater than age of universe), the cipher cannot be broken.

1- b) p asal ise $\phi(p) = p\text{-}1$ durumunu ispat ediniz. Euler Totient fonksiyonu nasıl kullanılır belirtiniz.
Cevap:

Euler totient of n, which is the number of positive integers less than n and relatively prime to n. Euler's Totient function Φ (n) for an input n is the count of numbers in {1, 2, 3, …, n-1} that are relatively prime to n, i.e., the numbers whose GCD (Greatest Common Divisor) with n is 1.

Euler fonksiyonu, Euler Fermat teoreminde de kullanılır. Şöyle ki:

$a^{\varphi(n)} \equiv 1 \pmod{n}$, *a* ile *n* aralarında asal ise. Dolayısıyla, $a^{\varphi(n)} - 1$, *n*'in bir tam katıdır.

Örneğin, $a^4 - 1$, $a = 1, 3, 7, 9$ için sırasıyla $0, 80, 2400, 6560$, *10*'un bir tam katıdır.

n	ϕ(n)	n	ϕ(n)	n	ϕ(n)
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

Tablo 6.6. 1-30 arası sayılar için ϕ(n) değerleri

$\phi(p) = p - 1$ where p is any prime number. We know that $gcd(p, k) = 1$ where k is any random number and $k \neq p$. Total number from 1 to p = p Number for which $gcd(p, k) = 1$ is 1, i.e the number p itself, so subtracting 1 from p $\phi(p) = p - 1$.

Examples:

$$\phi(5) = 5 - 1 = 4$$
$$\phi(13) = 13 - 1 = 12$$
$$\phi(29) = 29 - 1 = 28$$

---

2) RSA algoritmasını tanımlayıp, p=3, q=11, e=7 ve M=5 için açıklayınız.
Cevap:

n = 3 * 11 = 33
φ(n) = φ(33) = (3-1) * (11-1) = 20
1 < e < φ(n)
We should select an arbitrary number for **e** between 1 and φ(n)

- n and e used to generate public key

d = 1 mod φ(n)
let's assume d = 21

- d is used to generate private key

encryption:
c = M^e mod n
c = 5^7 mod 20 = 5, ciphertext is 5

decryption:
M = c^d mod n
M = 5^21 mod 20 = 5, plaintext is 5

---

3 –a) N tamsayının ondalık digitlerinin toplamı mod 9 da benzer olduğunu gösteriniz. Örnek: (16 mod 9 = (1 + 6) mod 9)
Cevap:

---

3 –b) p asal sayı ise, x^2 = 1 mod p'nin x = 1 mod p ve x = (-1) mod p çözümlü olduğunu gösteriniz.
Cevap:

---

4 –a) Simetrik şifrelemenin çalışma modları nelerdir? Output feedback ve counter modu karşılaştırnız?
Cevap:
-Electronic Code Book (ECB)
-Cipher Block Chaining (CBC)
-Counter (CTR)
-Output Feedback Mode (OFM)
In output feedback mode, each block is dependent on the previous encryption, so each time a block is changed all the blocks should be re-encrypted from the start. Counter method solves this problem since each block is independently encrypted. But requires a synchronous counter and if the synchronization is lost, recovery of plaintext is erroneous.

---

4 –b) Mac ve Hash fonksiyonu ne demektir? Collision resistance nedir?
Cevap:
It is a message integrity and authenticity method which combines hashing and MAC(message authentication code). It uses two keys to generate authentication code and appends it to the message. [m | h(k2 | (h(k1 | m))]
Two messages can have the same hash value. This is called a collision. Collision resistance is the capability of the hash functions to evenly distribute hashes to avoid collisions.

---

5 –a) Eliptik eğriyi ve çalışma yöntemini açıklayınız.
Cevap:
İşlemedi. 11. slayt konusu

---

5 –b) Kuantum kriptografik ne demektir? Hangi amaçlar için kullanılır?
Cevap:
İşlemedi. 12. slayt konusu

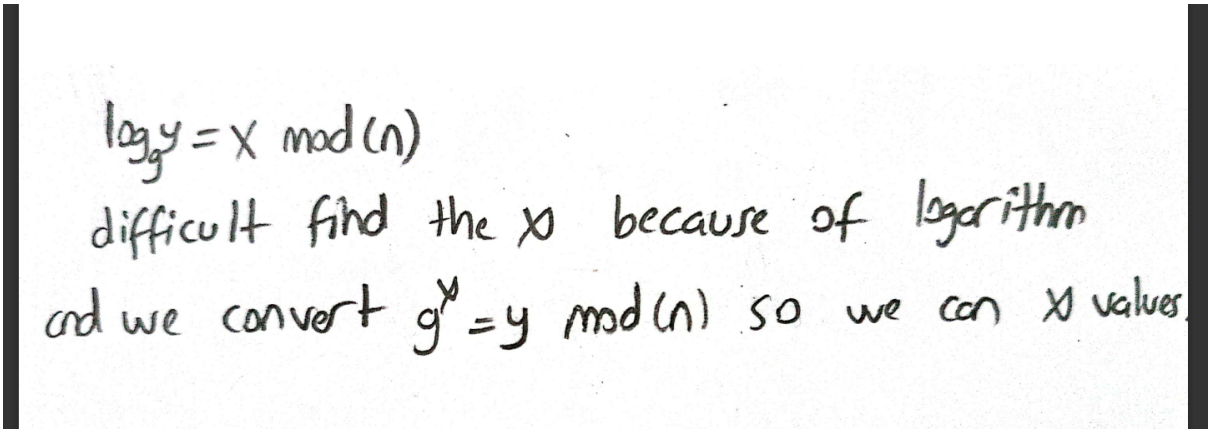
2020 Final

1.

a) Trap fonksiyonu ile oluşturulan ayrık logaritma problemi nedir? Kaç çeşit ayrık logaritma problemi vardır açıklayınız. (10p)
Cevap:

One way trap functions are not invertible,These are one-to-one functions. The discrete logarithm problem is based on the difficulty of inverting a logarithmic expression.

For example:



The harder the exponential expression is to find, the harder the discrete logarithm problem. Because the inverse of the exponential expression is done by applying the modulus.RSA and Diffie Helman are designed using the discrete logarithm

---

b) Sadece çıkışını (output) bildiğimiz kapalı kutu içerisinde bir şifreleme sistemi mevcuttur. Bu sistemin güvenli olduğunu nasıl anlarsınız? (10p)
Cevap:

By changing any byte in plain text, the changing number of bytes in the ciphertext is controlled. In case of a byte change, changing too many bytes in the ciphertext can give information about the security of the system. We call this the avalanche effect. Depending on each byte change in the plain text, we can say that the more bytes in the ciphertext, the more secure it is.

2.
Simetrik şifrelemede Çalışma Metotları ne için vardır, faydaları nelerdir? Output Feedback (OFB) ve Counter Modu (CTR) karşılaştırarak açıklayınız. (15p)
Cevap:

While symmetric encryption is an older kind of encryption, it is faster and more efficient than asymmetric encryption, which strains networks due to data capacity limitations and excessive CPU usage. Symmetric cryptography is commonly used for bulk encryption / encrypting massive volumes of data, such as database encryption, due to its superior performance and speed (relative to asymmetric

encryption). In the case of a database, the secret key may be used to encrypt or decrypt data exclusively by the database. The following are some examples of where symmetric cryptography is used:

- Payment applications, such as card transactions require the protection of personally identifiable information (PII) to prevent identity theft and fraudulent charges.
- Validations to ensure that the message's sender is who he says he is.
- Hashing or generating random numbers

Advantages of symmetric algorithms

Exceptionally safe

Symmetric key encryption can be highly secure when it employs a secure algorithm. As recognized by the US government, the Advanced Encryption Standard is one of the most extensively used symmetric key encryption schemes. Using ten petaflop machines, brute-force guessing the key using its most secure 256-bit key length would take about a billion years. Because the world's fastest computer, as of November 2012, runs at 17 petaflops, 256-bit AES is virtually impenetrable.

Speed

One of the disadvantages of public-key encryption methods is that they require very complex mathematics to function, making them computationally intensive. It's pretty simple to encrypt and decrypt symmetric key data, resulting in excellent reading and writing performance. Many solid-state drives, which usually are pretty fast, use symmetric key encryption to store data inside, yet they are still quicker than traditional hard drives that are not encrypted.

Acceptance

Because of their security and speed benefits, symmetric encryption algorithms like AES have become the gold standard of data encryption. As a result, they have enjoyed decades of industry adoption and acceptance.

Requires low computer resources

When compared to public-key encryption, single-key encryption uses fewer computer resources.

Minimizes message compromises

A distinct secret key is utilized for communication with each party, preventing a widespread message security breach. Only the messages sent and received by a specific pair of sender and recipient are affected if a key is compromised. Other people's communications are still safe.

OFB AND CTR DIFFERENCES:

- A single bit error in a block is propagated to all subsequent blocks. This problem is solved by OFB as it is free from bit errors in the plain text.(OFB)
- Parallel execution of encryption is possible as outputs from previous stages are not chained.

3.

a) Gizli ve Açık anahtar kullanılarak anahtar değişim(key excahnge) işlemi nasıl yapıldığını açıklayınız. Oturum anahtarı ve Diffie-Hellman anahtar değişim algoritmalarının nasıl çalıştığını açıklayınız. (10p)

Cevap:

Encryption is a process to change the form of any message in order to protect it from reading by anyone. In Private-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.

Public Key Encryption is based on public and private key encryption techniques. It uses two different key to encrypt and decrypt the message. It is more secure than the private key encryption technique but is much slower.

A session key is a single-use symmetric key used for encrypting all messages in one communication session.

---

b) 92 farklı ASCII karakterinden oluşan bir kümedeki elemanlar kullanılarak oluşturulmuş 8 hanelik bir şifre mevcuttur. Saniyede 6.4 milyon işlem yapma kapasitesine sahip bir bilgisayar ile bu şifreyi kırmak en kötü ihtimalle ne kadar zaman alacağını hesaplayınız. (10p)
(Not: Her bir şifre denemesi bir bilgisayar işlemine tekabül etmektedir.)
Cevap:

(92^8 * 2^8) / 6400000

4.
a) EBOB(m,n) = 1 ise φ(m,n) = φ(m) * φ(n) olduğunu gösteriniz. (10p)
Cevap:

not : φ(n), n sayısının aralarında asal olduğu n'den küçük sayı miktarını gösteriyor. mesela φ(10) için 10 dan küçük aralarında asal olduğu sayılar 1, 3, 7, 9 yani φ(10) = 4 eğer sayı asalsa mesela φ(11), o zaman direkt olarak asal sayıdan 1 çıkarılabilir φ(11) = 10

cevap

if GCD(m,n) = 1, then m and n are coprime(relatively prime), which means that there are no prime factors that they share in common.

If we consider the set of integers {1, 2, 3, ..., mn}. This set can be partitioned into two disjoint subsets: the integers that are relatively prime to m, and the integers that are not relatively prime to m. The same can be done for the integers in the set that are relatively prime to n.

Let S1 be the set of integers in {1, 2, 3, ..., mn} that are relatively prime to m, and let S2 be the set of integers in {1, 2, 3, ..., mn} that are relatively prime to n.

Note that the intersection of S1 and S2 is the set of integers in {1, 2, 3, ..., mn} that are relatively prime to both m and n. This set is exactly the set of integers in {1, 2, 3,

..., mn} that are relatively prime to mn, since m and n are coprime and there are no prime factors that they share in common.

Therefore, the number of integers in {1, 2, 3, ..., mn} that are relatively prime to mn is the same as the number of integers in the intersection of S1 and S2, which is the number of integers in S1 multiplied by the number of integers in S2.

This means that φ(mn) = |S1| * |S2| = φ(m) * φ(n).

Thus, if GCD(m,n) = 1, then φ(mn) = φ(m) * φ(n).

---

b) Çarpanları asal sayılardan (p,q) oluşan bir N sayısı bilinmektedir. (p-1)(q-1) işleminin de sonucu bilindiğine göre N sayısının kolaylıkla çarpanlara ayrıldığını gösteriniz. (10p)
Cevap:

- **n = pq**
- **φ(n) = (p-1)(q-1)**
- **φ(n) = pq - (p+q) + 1**
- **φ(n) = n - (p+q) + 1, this yields to**
- **(p+q) = n - φ(n) + 1, we know that q = n / p, so**
- **p + (n/p) = n - φ(n) + 1, multiply with p both sides**
- **p(p + (n/p)) = p(n- φ(n) + 1)**
- **p^2 + n = p(n- φ(n) + 1) and then a quadratic equation for p;**
- **p^2 - (n - φ(n) + 1)p + n = 0, after this we can find q as well.**

5.
a) Kriptoanaliz nedir, açıklayınız. Lineer (Doğrusal) Kriptoanaliz yöntemleri nelerdir? (10p)
Cevap:

Cryptanalysis is the study and practice of breaking cryptographic codes and ciphers in order to access the information they protect. It is a field that involves analyzing and understanding the algorithms and techniques used to encrypt and decrypt data, and then using that knowledge to identify weaknesses and vulnerabilities that can be exploited to gain unauthorized access.

Linear cryptanalysis methods are a specific type of cryptanalysis that involves studying the linear relationships between the input and output of a cryptographic algorithm. These methods often focus on analyzing the patterns that emerge when large amounts of encrypted data are analyzed, with the goal of identifying trends and

regularities that can be used to break the code. These techniques can be effective against certain types of ciphers, such as block ciphers, and can be used to quickly and efficiently break encryption algorithms that are otherwise considered secure

---

b) Sayısal İmza nasıl oluşturulur? Sayısal imzaların nasıl doğrulandığını açıklayınız. (15p)
Cevap:

A digital signature is created by using a combination of a private key and a hashing algorithm. The private key is a unique code that is only known to the person creating the signature, and the hashing algorithm is a mathematical function that converts the original message or document into a fixed-length code known as a hash.

To create a digital signature, the person creating the signature uses their private key to encrypt the hash of the original message or document. This creates a unique digital signature that is attached to the original message or document.

To verify a digital signature, the recipient of the message or document uses the public key, which is freely available, to decrypt the digital signature. This produces the original hash of the message or document, which is then compared to a newly-generated hash of the original message or document. If the two hashes match, then the digital signature is verified as genuine.
