Advaitha Jayakumar
04 3BIT

ASSIGNMENT - I

Q1 Prime Factorization by trial division method

Ans The trial division method to check whether a number is a prime or not. Prime factorization by trial division is a method of finding the prime factors of a number by repeatedly dividing it by prime numbers until only prime factors remain.

Here are the steps

1. Start with the smallest prime number 2.
2. Divide the number to be factored by 2. If it is divisible by 2, write down 2 as a factor and divide the result by 2. Repeat this step until the result is not divisible by 2
3. Move on to the next prime number, which is 3. Divide the result obtained in step 2 by 3. If it is divisible by 3, write down 3 as a factor and divide the result by 3. Repeat this step until the result is not divisible by 3.
4. Continue this process with the next prime number, 5 and repeat with each successive prime number until the result is 1.
5. The prime factor of the original number are the prime numbers that were written down as factors in steps 2-4.

For example let's find the prime factors of the number 56 using the trial division method.

1. Start with 2.
2. 56 divided by 2 is 28, which is divisible by 2. Write down 2 as a factor and divide 28 by 2 to get 14.
3. Move on to 3. 14 is not divisible by 3
4. Move on to 5. 14 is not divisible by 5
5. Move on to 7. 14 divided by 7 is 2, which is divisible by 2. Write down 7 as a factor and divide 2 by 2 to get 1
6. The prime factor of 56 are 2, 2, 2 and 7.

Note that we continue with the division process even if a factor is repeated as in the case of the three 2s in the example above.

This is because each division by 2 reduce the number further and we want to capture all the factors.

Q2 Chinese Reminder Theorem

Chinese Remainder Theorem is a mathematical theorem that deals with finding a solution to a system of congruence. It states that eg we have a system of congruence of the form:

$x = a_1 \pmod{m_1}$
$x = a_2 \pmod{m_2}$
...
$x = a_i \pmod{m_i}$

where the values of $m_1, m_2, \ldots, m_i$ are pairwise relatively prime. Then there exist a unique solution for $x \pmod{m_1 m_2 \ldots m_i}$.

To find the solution, we can use the following algorithm:

1. Compute $M = m_1 m_2 \ldots m_i$, the product of all the moduli
2. For each $i = 1, 2, \ldots, i$, compute $M_i = M/m_i$.
3. For each $i = 1, 2, \ldots, i$ compute the inverse of M_i modulo m_i. This can be done using the extended euclidean algorithm
4. The solution is given by $x = \Sigma a_i M_i r_i \pmod{M}$, where r_i is the inverse of M_i modulo m_i.

For example let's solve the system of congruence

$x = 2 \pmod 3$
$x = 3 \pmod 5$
$x = 2 \pmod 7$

1. Compute $M = 3 \times 5 \times 7 = 105$
2. Compute $M_1 = 105/3 = 35$, $M_2 = 105/5 = 21$, $M_3 = 105/7 = 15$
3. Compute the inverse $r_1 = 2, r_2 = 1, r_3 = 1$ (since $35 \times 2 = 1 \pmod 3$, $21 \times 1 = 1 \pmod 5$ and $15 \times 1 = 1 \pmod 7$).
4. The solution is $x = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \pmod{105}$
   $= 23$.

Therefore the unique solution to the system of congruence is
$x = 23 \pmod{105}$

5. Explain the cipher properties

Ans A cipher is a mathematical algorithm used to encrypt plaintext to create ciphertext. The security and effectiveness of a cipher is based on its properties. Here are the most important properties of a cipher.

1. Confidentiality: A good cipher should ensure confidentiality, meaning that only the intended recipient should be able to read the message. The cipher should be designed in such a way that an attacker cannot easily obtain the plaintext from the ciphertext.
2. Integrity: A cipher should ensure integrity, meaning that the recipient can verify that the message has not been altered or tampered with during transmission. This is typically done by adding a message authentication code (MAC) or a digital signature to the message.
3. Authentication: A cipher should ensure authentication, meaning that the recipient can verify the identity of the sender. This is typically done by adding a digital signature to the message
4. Non-repudiation: A good cipher should ensure non-repudiation meaning that the sender cannot deny having sent the message. This is typically done by adding a digital signature to the message.
5
6. Key ~~strength~~ distribution: A good cipher should ensure secure key distribution, meaning that the key should be shared only between the sender and the recipient and not disclosed to any third party.
7. Key strength: A good cipher should ensure that the key is strong enough to resist attacks. This means that the key should be long and complex enough to make brute force attacks impractical
7. Speed and efficiency: A good cipher should be fast and efficient meaning that it should be able to encrypt and decrypt messages

quickly and use minimal resources.

Overall, a good cipher should provide a balance between security and usability, ensuring that the message is both protected and easily accessible to the intended recipient.

Q4. Explain Confusion and Diffusion

Confusion and diffusion are two important concepts in cryptography that were introduced in cryptography that were introduced by Claude Shannon the father of modern cryptography.

1. Confusion: Confusion refers to the process of making the relationship between the plaintext and the ciphertext as complex as possible. In other words the same plaintext should not produce the same ciphertext. This is achieved by using complex mathematical algorithms, such as substitution, permutation or S-boxes, which scramble the plaintext in a way that is difficult to predict. Confusion is intended to ensure that an attacker cannot determine the relationship between the plaintext and the ciphertext even if the attacker has access to the ciphertext and the encryption algorithm.

2. Diffusion: Diffusion refers to the process of spreading the influence of each plaintext bit over many ciphertext bits. This means that a small change in the plaintext should cause a large change in the ciphertext. Diffusion is achieved by using mathematical algorithms such as transposition, which reorders the bits or blocks of the plaintext in a way that is difficult to predict. Diffusion is intended to ensure that an attacker cannot easily detect patterns or redundancies in the ciphertext that could help them determine the plaintext.

Both confusion and diffusion are important in creating a strong and secure cryptographic systems. Confusion ensures that the relationship between the plaintext and ciphertext is complex while diffusion ensures

that small changes in the plaintext have a large effect on the ciphertext Together these techniques make it difficult for an attacker to analyze the ciphertext and determines the plaintext without knowledge of the encryption algorithm and key.