TBC-503 END-2021-22.pdf

17 October 2022 19:15

TBC-503 END-2021-...

Ans 5 (c) Explain Message Digest 5 (MD5)

MD5 was developed by Ron Rivest in 1991. It is a cryptographic hash function algorithm that takes input message of variable length and convert it into output of fixed length (16 bytes).

Output of MD5 is always 16 bytes * 8 → 128 bits.
It is fast and secure and used for message authentication.

Working → original message → 1000 bits.

① Padding → In the first step we add padding bits in the original message. Total length of the message is 64 bits less than exact multiple of 512.

1000 bits + 472 bits → 1472 bits
64 bit less than 1536 (512 * 3)

② Appending → We append original length modulo 64

1000 mod 64 → 1536 bits
+ 1472 bits

③ Splitting → Splitting the result in 512 bit blocks

1536 → Block 1 {512 bits}, Block 2 {512 bits}, Block 3 {512 bits}

④ Initializing chaining variables → Initialize 4 chaining variables (32 bits each)

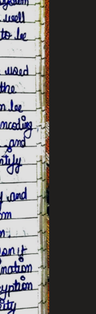
A
B
C
D

⑤ Process Blocks
→ copy chaining variables {A → a, B → b, C → c, D = d}
→ divide 512 bits block into 16 (32 bit) blocks
→ 4 rounds.

16 subblocks — const t[]
→ one round
a b c d

MD5 operation

$$a = b + ((a + Process(b,c,d) + M[i] + T[k]) <<< shift)$$



Advantages.
① Faster
② Generates strong digest of 16 bytes
③ Low memory required

Disadvantage
① Same hash function for different values of input
② Insecure than SHA
symmetric nor asymmetric algorithm

MIME (Multipurpose Internet Mail Extension) is a standard that was developed to allow the exchange of various types of electronic media, such as texts, audio, video and images, through mail or other Internet protocols. MIME uses a system of "Content-Type" headers to identify the type of content as well as its format being transmitted and allows the content to be encoded and transmitted as a part of the message.
MIME is not directly related to cryptography, but it can be used in combination with cryptographic techniques to secure the transmission of electronic media. For example, MIME can be used to transmit encrypted messages or files, by encoding the encrypted content as the part of MIME messages and using the appropriate "Content-Type" headers to identify the encrypted content.
In this way, MIME can help to ensure the confidentiality and integrity of the transmitted content, by protecting it from unauthorized access or tampering during transmission.
However, it is important to note that MIME alone doesn't provide strong security and should be used in combination with other cryptographic techniques, such as encryption and digital signatures, to provide a comprehensive security solution.

Digital signatures → A digital signature is a special type of code that is generated using a private key, and can be used to verify the authenticity of the message. When the message is signed using a digital signature, it can be verified by anyone who has the corresponding public key. Digital signatures are often used to ensure integrity and authenticity of electronic documents.

Hash Functions → A hash function is a mathematical function or algorithm that takes an input (called a message) and produces a fixed size output (called a "hash" value or "message digest"). Hash functions are only used to verify the integrity of a message by generating unique hash value for each message. If that message is later modified, the hash value will never match. Due to avalanche effect, allowing the receipient to detect if the message has been tampered with.

Fermat's Theorem and Euler's Theorem are two important theorems in number theory that are related to number theory and the concept of congruences.

Fermat's Theorem (Fermat's Little Theorem)

If p is prime number & a is any integer not divisible by p

$$\Rightarrow a^{(p-1)} \equiv 1 \bmod p$$

where

$$\frac{a^{(p-1)}}{p}, \text{ remainder} = 1$$

p = 7
a = 3, $(3)^{(7-1)} \Rightarrow 3^6 \equiv 1 \bmod 7$

Fermat's Theorem is often used in cryptography to test primality of any number, as it is quick way to find a number is either prime or composite.

Euler's Theorem

If p is a prime number, another integer a, a and p are co-prime

$$\Rightarrow (a)^{(phi(p))} \equiv 1 \bmod p$$

if p = 7 phi(7) = 6
a = 3, $(3)^{(phi(p))} \equiv 1 \bmod 7$, where phi(p) is euler's totient function.
$\hookrightarrow 3^{(6)}$

Euler's theorem is often used in cryptography to compute modular exponentiation efficiently, as it used to reduce exponentiation to be reduced modulo phi(p) without affecting result.

Euler's Totient

phi(p) → counts number of integers less than p, where i, p are coprime.
phi(7) = 6, coprimes of 7 → {1, 2, 3, 4, 5, 6}

Public key cryptosystems

Public cryptosystems are cryptographic systems that use a public key for encryption, allowing anyone to send encrypted messages to owner of the corresponding private keys. Public key cryptosystems are based on a number of principles, including:
① Asymmetric key encryption → Public cryptosystems are always implemented using a pair of keys, one which is used for the encryption (public key) and the other is used for decryption (private key). The keys are related but it is practically impossible to derive private key back from public key.
② Public key distribution → The public key is made available to anyone who wants to send an encrypted message to the owner of the private key. No need to exchange private keys between sender & receiver.
③ Key management → The private key must be kept secure & secret as it is only way to decrypt the messages for corresponding public key. Therefore the key management is essential.
④ Key Revocation → If the private key is compromised under any circumstances, the key needs to be replaced and hence the public key would be revoked and replaced with a new key.
⑤ Digital Signatures → Public cryptosystems can also be used to create digital signatures, which are used to verify authenticity and integrity of electronic messages or documents. Digital signatures use private key to sign any message & public key is used to verify the signature.
These principles form the foundation of public cryptosystems, and are essential for ensuring the security.