* FAQ's —

1. What is the important aspect that establishes trust in digital signatures?

→ If a sender & receiver know and trust each other, they can simply exchange public keys & establish secure data transmission, including authentication & encryption.
- But under normal circumstances, parties needing secure data transmissions have no foundation for trusting the identity of each other.
- Each needs a third party, whom they both trust, to provide proof of their identity.
- Such certificate authorities provide foundation by giving unique digital signature certificate to each user, that establishes trust between identities of both sender & receiver.

2. What is a Digital Signature Certificate (DSC)? Why do I need a DSC?

→ A digital signature certificate (DSC) is an electronic document that contains the Digital Signature of the certificate-issuing authority, binds together a public key with an identity & can be used to verify a public key belongs to a particular person or entity.
- DSC serves as a proof of identity of an individual or organization for a certain purpose on online/computer. DSC can be presented electronically to prove your identity, to access information or services on internet or to sign certain documents digitally manually.

3) How does a DSC work? Where can I purchase DSC?

Ans – A unique digital fingerprint (hash) of a document is created using any hashing algorithm.
– Then hash is encrypted using signer's private key.
– Encrypted hash & signer's public key ~~are appended~~ are combined into a digital signature, which is then appended to the document.
– DSC Applicants can directly approach Certifying Authorities ~~and~~ and issue a DSC using Aadhar eKYC authentication. A licensed CA issues Digital Signature.
– Some CAs are National Informatics Center (NIC), IDRBT CA, SafeScrypt CA services, E-MUDHRA, ~~etc.~~ (n) code solutions CA, TCS, CDAC, NSDL, Capricorn.

4) What are different classes of DSCs?

Ans → Different classes of DSCs are-

Class 2 : Here, the identity of a person is verified against a trusted, pre-verified database.

Class 3 : This is the highest level where the person needs to present himself or herself in front of a Registration Authority (RA) & prove his/her identity.

5) What is difference between digitally signing & encrypting an email?

→ Encrypting an email protects the privacy of the message by converting from plain text to cipher text. Only the recipient who has private key that matches the public key you used to encrypt the message can decipher the message.

- By digitally signing a message, you apply your unique digital mark to the message. The digital signature includes your certificate & public key. This information proves to the recipient that you signed the contents of the message & not an impostor, & that the contents have not been altered in transit.

6) What actually happens when I digitally sign any transaction?

→ - Transforming a process to make it entirely electronic requires securing & giving legal value to the transactions involved.

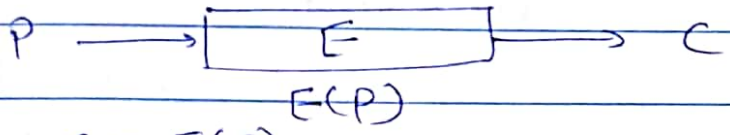
- Hence, secure & legally binding transactions are necessary in mobility when transaction is going on between two parties.

- Digitally signing any transaction generates a legally-binding proof of transaction, admissible in the event of a dispute.

1. FAQ's :-

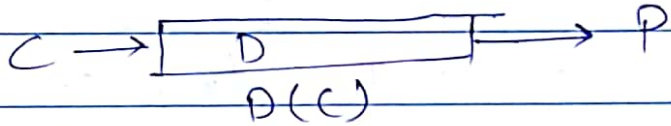
1. What is encryption & decryption of data?

Ans- The process of converting the plain text message to cipher text message is known as encryption.
Let, P is plaintext, E is encryption & C is cipher text.
If we perform E on P we get C.



i.e. $C = E(P)$.

The process of restoring the plain text from the cipher text message is known as decryption or process of converting ciphertext message into plaintext message is called as decryption.
Let, C be ciphertext, D is decryption & P is plaintext.
If we perform D on C it results in original P.



i.e $P = D(C)$.

2. How can Caesar Cipher be cracked?

Ans- There are 2 cases -

(i) If attacker does not know encryption technique then using techniques such as frequency analysis can be used to crack the cipher & find the key.

(ii) If attacker knows that Caesar Cipher is used then brute force attack can be used to find the key as there are only 25 shift values possible in case of Caesar cipher technique.

3) What is the importance of substitution boxes (S-boxes) & permutation box (P-box) in DES?

Ans- S-box is a basic component of symmetric key algorithms like DES which performs substitution.
- In S-box substitution 48-bit input that consist of 48-bit key XORed with 48-bit expanded right plaintext, is converted in 32-bit output.
- 32-bit output from eight S-boxes is then permuted, so that on the next round the output from each S-box immediately affects as many others as possible. The 32-bits are permuted by replacement of each bit with another bit in specified table called as P-box permutation.

4) What is difference between stream & block cipher?

Ans→

Basis for comparision	Block Cipher	Stream Cipher
① Basic	Converts the plain text by taking its block at a time	Converts the text by taking one byte of plain text at a time
② Complexity	Simple design	Complex Comparatively
③ No of bits used	64-bits or more	8 bits
④ Confusion & Diffusion	Uses both	Uses Confusion only
⑤ Algorithm modes used	ECB(Electronic Code Book) CBC(Cipher Block Chaining)	CFB(Cipher Feedback) OFB(Output Feedback)
⑥ Reversibility	Reversing encrypted text is hard	Uses XOR to encrypt that can be easily reversed to plaintext
⑦ eg Example	Feistel Ciphers	Vernam Cipher

5) What is the most secure way to design the forgot password feature?

s- By using a recovery phone number or email id.

- If user click forgot password then take input of user email id first.
- Then ask for the recovery mobile no./email id.
- If recovery details match then send an OTP (One time password) to recovery mobile no/ email id.
- If OTP is verified then only ask user to enter new password & verify it and hence, change the password successfully.

Assume known one secret key.

* FAQ's:

1) What security properties should a good hash function exhibit?

- The hash value is fully determined by the data being hashed.
- All input data must be used uniform distribution of data scores across entire set of possible values.
- Different hash value for same string.

2) What is MAC? Differentiate MAC & MD.

- MAC sometimes known as a tag is short piece of information used to authenticate a message.
- 2 Basic steps: Building a tag & verifying a tag.

Basis of Comparision	MD	MAC
Integrity	Yes	Yes
Authentication	No	Yes
Non-repudiation	NO	NO
Kind of keys	none	symmetric keys

A hash of the message, if appended to the message itself, only protects against accidental changes to the message, as an attacker who modifies the message can simply calculate a new hash & use it instead of the original one. So this only gives integrity.
A MAC protects against message forgery by anyone who doesn't know the secret key.

3) Compare MD5 & SHA1.

Ans →

Basis of comparision	SHA1	MD5
(i) Size of message in bits	160	128
(ii) Cryptanalysis attack ~~speed~~	Vulnerable	Not Vulnerable
(iii) Speed	Slow	Fast
(iv) Number of steps	80	64
(v) Buffer size in bits	160	128

4) Compare various version of SHA.

Ans →

Basis of Comparision	SHA-0	SHA-1	SHA-256/224	SHA-512/384
(i) Size of message in bits	160	160	256/224	512/384
(ii) Size of internal state in bits	160	160	256	512
(iii) Size of block in bits	512	512	512	1024
(iv) Length of message	$2^{64}-1$	$2^{64}-1$	$2^{64}-1$	$2^{128}-1$
(v) Size of word	32	32	32	64
(vi) No. of steps	80	80	64	80
(vii) Collision	Yes	2^{63} attack	Not yet	None yet

* FAQ's:

1) Enlist various algorithms used for primality testing.

Ans- Various algorithms used for primality testing are-
(i) Miller-Rabin Primality Test.
(ii) AKS primality test.
(iii) Fermat primality test.
(iv) Frobenius primality test.
(v) Pocklington Primality Test.
(vi) Elliptic curve Primality Test.

2) What are application of primality tests?

Ans- (i) Cryptography schemes such as RSA algorithm.
(ii) Computational number theory.
(iii) Information science
(iv) Computer science.

3) Demonstrate the Miller Rabin test for any large number & show the steps.

Ans- To determine if $n = 221$ is prime

$\therefore n-1 = 220 = 2^2 \times 55$

$\therefore s = 2$ & $d = 55$

Select a random number such that $1 < a < n-1$

Let $a = 174$

$a^{2^0 \cdot d} \bmod n = 174^{1 \times 55} \bmod 221 = 47 \neq 1, n-1$

$a^{2^1 \cdot d} \bmod n = 174^{110} \bmod 221 = 220 = n-1$

Since $220 \equiv n-1 \bmod n$, either 221 is prime, or 174 is a ~~strong~~ strong falsifier for 221.

Consider $a = 137$

$a^{2^0 \cdot d} \bmod n = 137^{55} \bmod 221 = 188 \neq 1, n-1$

$a^{2^1 \cdot d} \bmod n = 137^{110} \bmod 221 = 205 \neq 1, n-1$

∴ 137 is a witness for compositeness of 221,
& 174 was in fact a strong falsifier.