18/11/22

UNIT - 3.

Assignment - 3.

PART-A

Ques1:- If A and B want to communicate securely with each other, B must not know?

Ans:-

Ques2:- If the sender encrypts the message with her private key, it achieves the purpose of

Ans:- b) Confidentially and Authentication

Ques3:- When two different message digests have the same value, it is called as:-

Ans:- b) Collision

Ques4:- To verify a digital signature, we need the

Ans:- b) Sender's public key

Ques5:- To decrypt a message encrypted using RSA, we need the

Ans:- c) Receiver's private key

Ques6:- ____ are required to conduct commercial

transactions over the Internet.

Ans:- c) digital signature

Ques 7:- A digital certificate binds a user with

Ans:- b) The user's public key

Ques 8:- A can issue digital certificates.

Ans:- a) CA

Ques 9:- To solve the problem of trust, there is used.

Ans:- c) private key

Ques 10:- RSA stands for

Ans:- b) Rivest, Shamir, Adleman

Ques 11:- In asymmetric key cryptography although RSA can be used to encrypt and decrypt actual messages it is very slow if the message is.

Ans:- b) long

Ques 12:- Public key encryption uses or creates ___ in its algorithm.

Ans:- d) All of these answers are correct

Ans 12:- Using Rivest, Shamir, Adleman cryptosystem with $p = 7$ and $q = 9$. Encrypt $M = 24$ to find ciphertext. The ciphertext is:

Ans:- c) 114

Ans 14:- RSA algorithm is ___ cryptography algorithm.

Ans:- b) Symmetric

Ans 15:- Private key algorithm is used for ___ encryption and public key algorithm is used for ___ + ___ encryption.

Ans:- a) message, session key.

PART-B

Ans 1:- What are the disadvantages of asymmetric cryptography.

Ans:-
- It is slow process compared to symmetric cryptography
- If an individual loses his private key, he can't decrypt the messages he receives.
- If a malicious actor identifies a person's private key, the attacker can read that individuals message.
- Public key's are not authenticated, no one can ensure a public key belongs to the person specified. Consequently, users must verify that their public keys belong to them.

POPU

Page No.
Date : / /

Ques2:- Mention any one technique of attacking RSA.

Ans:- Plain Text Attack :- Plain text attacks are classified into three categories.

1) Short message attack
2) Cycling attack
3) Unconcealed message attack.

Ques3:- What primitive operations is used in RC5?

Ans:- There are three primitive operations:
1) integer addition
2) bitwise XOR - (exclusive - OR)
3) variable rotations.

Ques4:- What are the properties a digital signatures should have?

Ans:- 1) Authenticity
2) Unforgeability
3) Non-reusability
4) Non-repudiation
5) Integrity.

Ques5:- Differentiate between Asymmetric cryptography and Symmetric cryptography.

Ans:-	Symmetric cryptography	Asymmetric cryptography
1)	There is only one key is	There are a group of prim

	Symmetric	Asymmetric
	used between sender and receiver.	is used between sender and receiver (public and private key).
2)	It is effective as the technique is recommended for high amount of data.	It is inefficient as this technique is used for short messages.
3)	The length of key used is frequently 128 or 256 bits, based on the security level.	The length of the key much higher such as the recommended RSA key size is 2048 bits or higher.

PART-C

Ques1:- What is the Real crux of RSA?

Ans:- The Real crux of RSA algorithm :-
The knowledge of the public key does not reveal the secret key.

Ques2:- What is the important aspect that establishes trust in digital signatures.

Ans:- A digital signature - a type of electronic signature - is a mathematical algorithm routinely used to validate the authenticity and integrity of a ~~message~~ message. Digital signatures create a virtual

fingerprints, that is unique to a person or entity and are used to identify users and protect information in digital messages or documents.

Integrity :-
The digital signature preserves the integrity of a message because, if any malicious attack intercepts a message and partially or totally changes it then the decrypted message would be impossible.

Authentication :-
We can use the following reasoning to show how the message is authenticated, if a intruder (user X) sends a message pretending that it is coming from someone else (user A) user X uses her own private key to encrypt the message. The message is decrypted by using the public key of user A. Therefore this makes the message unreadable.

Non-Repudiation :-
Digital signature also provides non-repudiation if the sender denies sending the message then the private key corresponding to the public key is tested on the plaintext, if the decrypted message is the same as the original message then we know that the sender has sent the message.

POPU

Page No.
Date: / /

Ques3:- Which two type of key does asymmetric cryptography use.

Ans:- Asymmetric encryption uses a mathematically related pair of keys for encryption and decryption: a public key and a private key.

A public key is a cryptographic key that can be used by any person to encrypt a message so that the it can only be decrypted by the intended recipient with their private key.

A private key also known as a secret key -- is shared only with key's initiater.

Ques4:- What is the role of a CA and a RA? Name the four key steps in the creation of a digital certificate.

Ans:- The role of a CA:-

Certificate authority (CA): The certificate authority is a third party that verifies a person's identity. It does so by either generating a public / private key pair for them or correlates an existing key provided by that person. Once a person's identification is verified, the CA issues a digital certificate. The digital certificate can be used to validate that person by public key.

Registration Authority (RA):- The RA is an intermediate

entity between end users and the CA which assists the CA in its day-to-day activities. The RA commonly provides the following services:-

- Accepting and verifying registration information about new users.
- Generating keys on behalf of the end users.
- Accepting and authorizing requests for key backup and recovery.
- Accepting and authorizing the requests for certificate revocation.

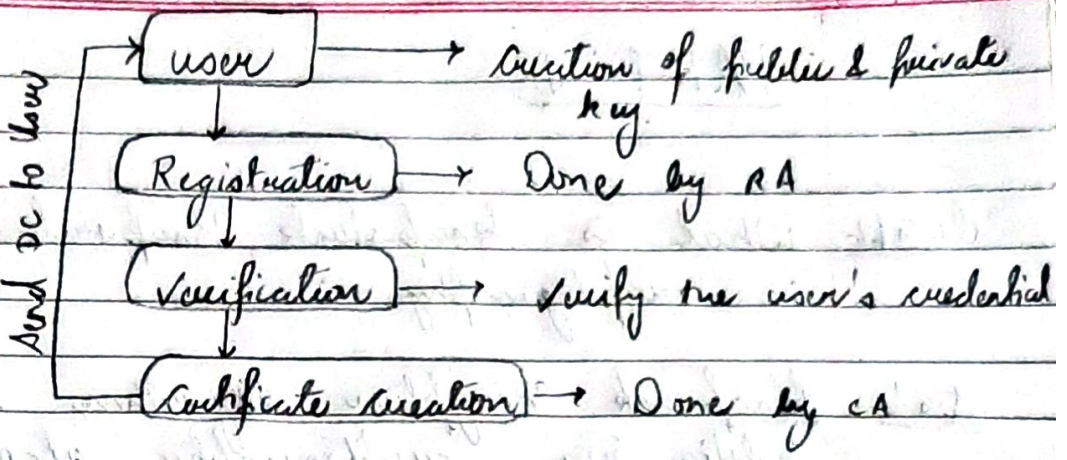
Steps of creating Digital Certificate:-

1) Key Generation :- Key generation is done by either users or registration authority. The public key which is generated is sent to the registration authority and private key is kept secret by user.

2) Registration :- In this step the registration authority registers the users.

3) Verification :- After the registration process complete, RA identifies the users credential

4) Certificate Creation :- In this step the details and sent to certificate authority by registration authority who creates the digital certificate and give it to users and also keeps a copy to itself.



Ques:- How do you calculate RSA algorithm.

Ans:- Calculation of RSA Algorithm:-

→ Choose two large prime numbers P and Q.
→ Calculate $N = P \times Q$
→ Choose the public key (i.e. the encryption key) E such that it is not an element of $(P-1) \times (Q-1)$.
→ Choose the private key (i.e. the decryption key) D including the following equation is true:-
$(D \times E) \bmod (P-1) \times (Q-1) = 1$
→ For encryption, calculate the cipher text (CT) from the plain text (PT) as follows:-
$CT = PT^E \bmod N$
→ Send CT as the cipher text to the receiver.
→ For decryption, calculate the plain text (PT) from the cipher text (CT) as follows:-
$PT = CT^D \bmod N$

POPU

PART- D

Ques1: What is ~~knapstack~~ Knapsack encryption algorithm in cryptography.

Ans:- Knapsack Encryption Algorithm is the first general public key cryptography algorithm. It is developed by Ralph Merkle and Martin Hellman in 1978. As it is a Public key cryptography, it needs two different keys. One is public key which is used for Encryption process and other one is Private key which is used for Decryption process. In this algorithm we will two different knapsack problems in which one is easy and other one is hard. The easy knapsack is used as the private key and the hard knapsack is as the public key. The easy knapsack is used to derived the hard knapsack.

For the easy knapsack, we will choose a "Super Increasing knapsack problem". Super increasing knapsack is a sequence in which every next term is greater than the sum of all preceding terms.

Ques2: Perform encryption and decryption using RSA Alg for the following:

$P = 5$, $q = 11$, $e = 17$, $M = 8$.

Ans:- $p = 5$, $q = 11$, $e = 17$, $M = 8$.

$N = p \times q = 5 \times 11 = 55$

$f(N) = (p-1)(q-1)$

$= (5-1)(11-1) = 40$

$D = (1 + k f(N)) / e$

$= (1 + 40k) / 17$

$= (1 + 40(-3)) / 17 =$ for $(k = -3)$

$= -119 / 17 = -7$

$D = -7 \pmod{40} = 33$

$C = M^e \pmod{n}$

$= 8^{17} \pmod{55} = 13$

$M = C^d \pmod{n}$

$13^{33} \pmod{55} = 22$