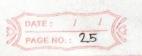
0:13 Using Rivest, Shamir, Adleman tryptosystem with P-7 and 9=9, Encrypt H=24 to find riphertent. The Tipherteat is. 1 de la contrata del contrata del contrata de la contrata del la contrata de la contrata del la contrata de la 0.14 RSA algorithm is - cryptography algorithm De met lais sammer Tantara all latinos des O15 Brivate key algorithm is used for - encryption and public key algorithm is used for + encryption. Section-B OI What are the disadvantages of asymmetric cryptogra D) It is islow process compared to symmetric cryptigraps
If an individual loses his private key, he can't decry--pt the menages he receives.



key, the attacker can great that individuals a 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. Mention any one technique of attacking RSA Plain Text Attack :-Plain text attacks are classified into three categories. 1) short menage attack 2) Cycling attack 3) Unconcealed menage attack. 0.3 What primitive operations is used in RCS? A> There are Three primitive operations: 1 Integer addition 21 bituise XOR-(exclusive -or) 3) variable rotations O.4 What are the proporties a digital signatures should have D) 1 Authenticity 2 Unforgentility 3) Non-re-wability 4 Non-repudiation 5) Integrity 0.5 Differentiate between Asymmetric Gyptography and symmetric Cryptography

	Symmetric Cnyptography	Asymmetric Cryptogeoph
	There is only one key is	There are a group of poly
	wed between sender and	is used between sendas
	receiver.	and receiver (public and
		poinate Rey
2)	It is effective as this technique	It is inefficient as this fel
	is secommended for high	que is itsed for short meraje
	amount of data.	O Company
31	The length of key used is -	The length of the key much
	frequently 128 or 256 bits, based on the sayuity level.	higher such as the recommended
	based on the sayify level.	RSA key size is 2048 bits on
		higher.
4)	It is also known as	It is also known as public
	symmetric key/secret	key or conventional public
	key cryptography	system.
	0 0 0 0	3.44.11
	Section - C.	son silining todal To
	Secretary of the second second	medic Capp sand CA
0.1	permitted special way	med to stage again the
Q·1	What is the Real	crux of RSA?
A-)	What is the Real The Real Trux of R	crux of RSA?
A-)	What is the Real The Real Trux of R The knowledge of the	crux of RSA? ISA -algorithm is: public key does not
A-)	What is the Real The Real Trux of R	crux of RSA? ISA -algorithm is: public key does not
A-)	What is the Real The Real Trux of R The knowledge of the reveal the secret Ke	crux of RSA?  LSA -algorithm is:  public key does not
A-)	What is the Real The Real Trux of R The knowledge of the reveal the secret Key What is the important	crux of RSA?  LSA -algorithm is:  public key does not
0.2	What is the Real The Real Trux of R The knowledge of the reveal the secret Key What is the important in digital signatures.	crux of RSA?  SA -algorithm is:  public key does not  respect that establishes trust
0.2	What is the Real The Real Trux of R The knowledge of the reveal the secret Key What is the important of in digital signatures. A digital signature -	cour of RSA?  ISA -algorithm is:  public key does not  respect that establishes trust  a type of electronic
0.2	What is the Real The Real Trux of R The Real Trux o	cour of RSA?  SA -algorithm is:  public key does not  spect that establishes trust  a type of electronic tical algorithm noutinely
Q.2	What is the Real The Real Trux of R The Real Trux o	crux of RSA?  SA -algorithm is:  public key does not  spect that establishes trust  a type of electronic tical algorithm routinely withenticity and integrity
Q.2	What is the Real The Real Trux of R The Real Trux of R The knowledge of The reveal the secret Key What is the important of in digital signatures. A digital signature— Signature—is a mathema used to validate the e	SA -algorithm is:  public key does not  spect that establishes trust  a type of electronic tical algorithm noutinely whenticity and integrity signatures create a
Q.2	What is the Real The Real Trux of R The Real Trux o	crux of RSA?  SA -algorithm is:  public key does not  spect that establishes trust  a type of electronic tical algorithm routinely whenticity and integrity signatures create a  t is unique ito a



users and project information in digital manages

Integrity!

The digital signature preserves the integrity of a message because, if any malicious attack intercepts a message and Portially our totally thanges it then the decrypted message would be impossible.

Authentication :-

we can use the following seasoning to show how the message is authenticated. if a intruder (user X) sends a message pretending that it is roming from someone else (user A), user X user her own private key to energyt the message. The message is decrypted by using the public key of user A. Therefore this makes the message ungradable

Non-Repudiation:

Jot

Digital signature also provides non-repudiation if the sender denies sending the merage then her private key corresponding to her public key is tested on the plaintent if the decrypted merage is the same as the original merage, then we know that the sender has sent the merage

OB Which two type of key does asymmetric tryptography use.