LIYANA ARACHCHIGE RANIL

JAVA SECURITY – CRYPTO API

1. Cryptography is used to either encrypt or decrypt sensitive information
2. JAVA cryptographic API provides a framework and implementations for ENCRYPTION , KEY GENERATION , KEY AGREEMENT and support for MESSAGE AUTHENTICATION CODE (MAC) algorithms
3. Support for ENCRYPTION included SYMMETRIC, ASYMMETRIC, BLOCK and STREAM Ciphers. Also it supports SECURE STREAMS and SEALED OBJECTS
4. Good Cryptography is based on the SECRECY of the KEY and not the ALGORITHM for security
5. A good ALGORITHM is one which can be publicly available and proved to be secure
6. Cryptography can be used to provide CONFIDENTIALITY , DATA INTERGRITY , AUTHENTICATION
7. The original data which is going to be fed in to a Cryptographic algorithm is know as plaintext while the protected or encrypted data is known as Cipher text
8. ENCRYPTION is the process by which plaintext can be made to Cipher text
9. DECRYPTION is the process by which Cipher text is made to be plaintext
10. There are two BASIC types of CRYPTOGRAPHIC systems , ASYMMETRIC and SYMMETRIC
11. SYMMETRIC key systems require both the sender and the receiver have the same key

12. ASYMMETRIC key systems use two key, PUBLIC and PRIVATE. User encrypt using PUBLIC key while it can only be decrypted using PRIVATE key
13. PUBLIC key is published widely while the PRIVATE key kept secret
14. PUBLIC KEY INFRASTRUCTURE or PKI'S is there to address the problem of trusting other person who publishes information. Hence another third part is involved in certifying the owner of such information
15. A Cipher is an ALGORITHM to render text or information encrypted and unreadable unless you have the cipher to DECIPHER it
16. SYMMETRIC ciphers are slower than SYMMETRIC ciphers
17. In SYMMETRIC key cryptography key exchange is a problem
18. There are two types of SYMMETRIC algorithms, STREAM and BLOCK
19. STREAM Ciphers operates on one BIT at a time
20. BLOCK ciphers break the information into blocks and encrypt those
21. A BLOCK Cipher encrypts data in FIXED size blocks
22. Mostly used BLOCK CIPHERS > **TRIPLE DES , AES**
23. SYMMETRIC CIPHERS > **AES / Rijndael, Blowfish,CAST5,DES,IDEA,RC2,RC4,RC6,Serpent,Triple DES , Twofish**
24. There are two method of breaking SYMMETRIC ENCRYPTION, Brute Force and Cryptanalysis
25. Brute Force is an attack in which each possibility is tried until a successful once is found

26. Cryptanalysis is an attack in which the cryptographic algorithm characteristic is used to deduce a plaintext or cipher text
27. ASYMMETRIC encryption uses different keys for encryption and decryption
28. It is very difficult to derive the decryption key from the encryption key
29. The encryption key is PUBLIC so that anyone can encrypt a message and send to the expected receiver
30. The decryption is kept PRIVATE
31. It is common to set up a key pair within a network so that each user has a PUBLIC and PRIVATE key
32. Some ASYMMETRIC algorithms allow process to work the opposite direction as well, a message can be encrypted with the private key and decrypted wit the corresponding public key (RSA is an example of such an algorithm)
33. Popular **ASYMMETRIC encryption** algorithms Reverst-Shamir-Adleman (**RSA**), Digital Signature Algorithm (**DSA**), Pretty Good Privacy (**PGP**) (Protocol based on ASSYMETRIC ALGORITHMS like IDEA, CAST or Triple DES for data encryption while RSA or **Diffie-Hellman(DH)**/DSS for key management and digital signatures. The RSA or DH public key is used to encrypt IDEA secret key as part of the message) , **DH (Diffie-Hellman Key exchange algorithm) , ECDSA** (Elliptic Curve DSA), **XTR**
34. HASHING is an special form of encryption in which for a given unique input it would create a fixed length output called HASH or MESSAGE DIGEST
35. HASHING most often uses ONE WAY ALGORITHMS
36. HASH collision means that two different messages having the same HASING VALUE

37. HASH algorithms takes a long strings as the input and creates a fixed length encrypted output known as MESSAGE DIGEST / DIGITAL FINGERPRINT / CHECKSUM / HASH CODES or HASH
38. Widely used cryptographic HASHING algorithms are SHA-1, SHA-2,MD4 , MD5 (Broken)
39. KEY AGREEMENT is a protocol by which two parties can establish the SAME CRYPTOGRAPHIC KEY without having the exchange any secret information
40. Message Authenticate Code (MAC) provides a way to check the INTERGRITY of information transmitted over or stored in an unreliable medium based on a SECRET KEY
41. MAC algorithms usually accept a SECRET KEY and the MESSAGE itself and output a MAC. This MAC value protects both message INTEGRITY and AUTHENTICITY
42. MESSAGE DIGEST is the HASH calculated using a given Message , and this MESSAGE DIGEST is SIGNED using PRIVATE KEY of the owner which makes the DIGITAL SIGNATURE and appended to the message it self as the DIGITAL SIGNATURE
43. Receiver of the Message would also have the SECRET KEY and can verify if the MAC is correct with the received message. This would enable message INTERGRITY
44. MAC values are different from DIGITAL SIGNATURES , since MAC value is generated using a SECRET KEY and verified against the SAME key
45. DIGITAL SIGNATURE is done using a PRIVATE KEY of a PUBLIC PRIVATE KEY PAIR. Which means only one person possesses the PRIVATE KEY and that does provide NON REPARDIATION.
46. A SALT is a random bits added at the end of a SECURE KEY
47. Sometimes SALT is used in generating MAC

48. PUBLIC KEY INFRASTRUCTURE is a set of hardware , software , people and policies to create , distribute , revoke DIGITAL CERTIFICATES
49. In Cryptography PKI is an arrangement that binds PEOPLE with DIGITAL CERTIFICATES by means of a CERTIFICATE AUTHORITY (CA)
50. X.509 is an ITU-T standard for PKI
51. in X.509 system a CERTIFICATE AUTHORITY issues a CERTIFICATE binding a PUBLIC KEY to a particular DISTINGUISE name
52. If some one needs a X.509 compliant PKI , PUBLIC CERTIFICAT E, he or she first needs to create a PRIVATE and PUBLIC KEY PAIR , generates a CERTIFICATE SIGNING REQUEST (CSR) with the PRIVATE KEY and send the CSR to a CERTIFICATE AUTHORITY (CA) who would SIGN the CSR with the CA'S PRIVATE KEY and issue a DIGITAL CERTIFICATE for the person
53. Using the requesters PRIVATE KEY , entire CSR request is signed before sending the request to a CA
54. A Cryptographic Provider in JAVA is referred to as a library which provides implementation of subset of JAVA CRYPTO API features
55. To install a new provider ,
    a. STEP1
       Add the provider to the list of approved providers. This can be done by editing the **java.security** file in lib/security directory , add the property
       security.provider.n=masterClassName

    b. STEP2
        i. Place a zip or jar in the classpath

ii. Supply jar file as a bundled or installed as an extension in the JRE itself

56. Providers may also be registered dynamically. For that they should have been given permission to call addProvider , indertProviderAt methods

57. JAVA provided necessary API for Cryptographic operations