Assignment No: 03

Computer Security

NAME: ASHFAQ AHMAD

Reg No: 19PWCSE 1795

Section: A

Submitted to:

Dr. Sadeeq Jan Sab

DCSE, UET Peshawar

Q: NO: 01

Explain the use of Digital signature with numerical example.

Digital Signature:

A digital signature is a method used to ensure (or) verify the authenticity and Integrity of a digital document or message it uses a set of mathematical algorithms to generate a unique code called a signature that is linked to original document or message. this signature is used to to verify the message or document has not been tampered and was sent by a person who claimes to have sent it.

→ The ~~recipient~~ sender create digital signature by using cryptographic algorithms and their Private key.

→ The reciever then verify digital signature by using Public key of sender.

P.T.O

Numerical example!

(1) Ali choose two large prime numbers, $p = 11$ & $q = 17$.

(2) Ali calculates $n = pq = 187$ an $\phi(n) = (p-1)(q-1) = 160$.

(3) Ali choose a public expenent $e = 7$ which is reliativily prime to $\phi(n) = 160$.

(4) Ali calculate a private exponent. such that

$$e \cdot d \bmod \phi(n) = 1$$

$$0 \leq d \leq n$$

formula

$$d = \frac{k \cdot \phi(n) + 1}{e} = 23$$

(5) Ali Public key and Private key.

$$KU = \{e, n\} = \{7, 187\}$$

$$KR = \{d, n\} = \{23, 187\}$$

(6) Ali want to send a message $m = 40$ to Hamza.

(7) Ali creates a signature, by using his private key.

$$S = m^d \bmod n = 40^{23} \bmod 187 = 167$$

(8) Ali send the message $m = 40$ signature $s = 167$ to Hamza

(9) Hamza Receives message $m = 40$ signature $s = 167$

(10) Hamza uses Ali public key$(e, n) = \{7, 187\}$ to verify signature.

$$m' = s^e \bmod n = 167^7 \bmod 187 = 40$$

(11) Ali compares $m = m' = 40$ and satisfies that message is authentic and not tempered.

Q2: Can hash function be used with digital Signature? explain advantage and disadvantage of Course.

Ans: Yes, hash function Can be used togather with digital signature. In fact, they are Commonely used in Combinition to provide an additional layer of Security.

A digital Signature alone ensures the authenticity and Integrity of a message but it doesn't guarantee ~~Cond~~ Confidentiality. Hash function can be used to encrypt the message before it is signed so the only recipient with correct decryption key can read it. This is called "digital Signature with Encryption" or "digital signature with message Recovery".

Advantages:

* Provide both confidentiality and Integrity.
* Prevent unauthorized parties from reading the message.
* Provide ~~ensurance~~ ensurance that message has not been tampered.
* Recever original message from Signature.

P e T p o

Disadvantages:

* Increase ~~comp~~ complexity of Encryption process.
* may be less efficient as compare to using digital signature or hash function alone.
* Increase the size of the message that needs to be transmitted. (both signature and encrypted message are sent).

— xx — xx — xx — xx — xx — x

Q.03: Does the Public key cryptographic algorithms resolve the key distribution issue? Why or why not.

Ans: Public key cryptography resolve the issue of Key distribution. b/c it uses a pair of keys one for encryption (Public key) other for decryption (Private key). the Public key can be freely distributed to anyone, and is used to Encrypt the message. the private Key is kept Secret by the owner, and is used to decrypt the message. this means that the sender doesn't need to have access to the receiver's secret key in order to Encrypt a message for them or simply Sender doesnot need to send any key with Encrypted message to the receiver for decryption.

Additionally, Public key cryptography only resolve the issue of key distribution for encryption and

P.T.O

decryption. it doesn't Resolve the issue of key distribution for authentication and Integrity. therefore it is often used in combinition with other cryptographic techniques to provide a complete Security Solution.

—xo ——xo ——xo ——xo

END of Assignment NO: 03