Information System Security 2020

SCS 2214

01 (a).

Crackers

* Active attempts to access sensitive resources and to discover system vulnerabilities (minor inconvinience to regolar users)

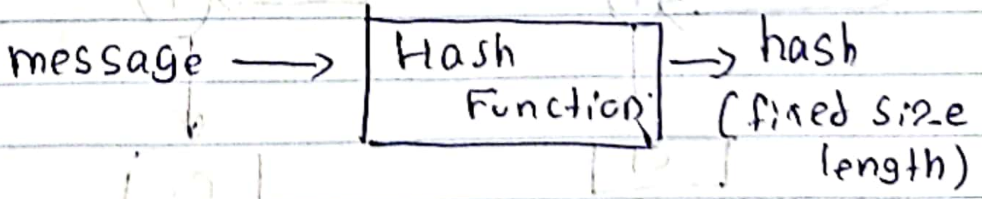
Criminals

* Active attempts to Utilize weakness in protection system in order to steal or destroy resources (Serious problems to regular users)

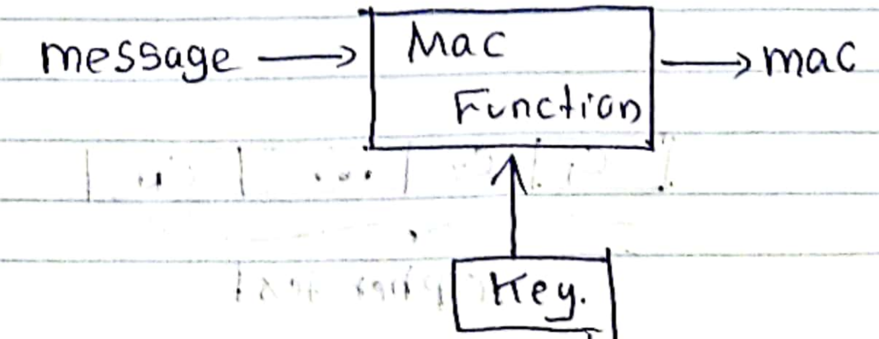
(b) Mac is simillar to ~~the~~ cryptographic hash, except it is based on a secret key

* Hashes are used to gurantee integrity of data
* MAC gurantee integrity and authenticate

Hash



MAC



(c). To make last block to fit the block size inserting Some dummy data to last block

* Receipient should have an understand on which block is dummy which block is not.

A	B	C					
41	42	43	05	05	05	05	05

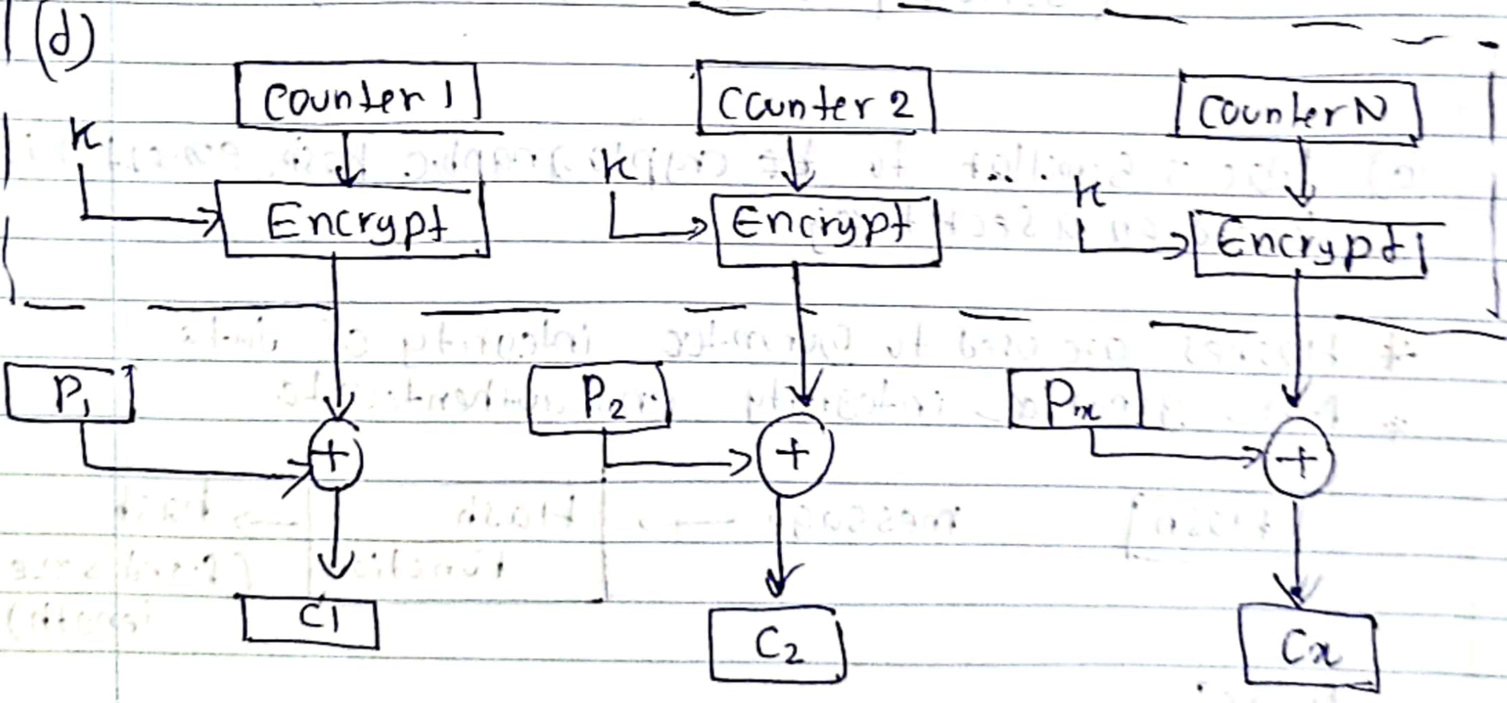
A	B	C	D				
41	42	43	44	04	04	04	04

A	B	C	D	E			
41	42	43	44	45	03	03	03

A	B	C	D	E	F	G	H
41	42	43	44	45	46	47	48

08	08	08	08	08	08	08	08

(d)



$O_i = E_K(i)$

$C_i = P_i \text{XOR} O$

$$\underbrace{C_1 \mid C_2 \mid \dots \mid C_N}_{\text{cipher text}}$$

- Simillar to OFB
- But encrypt counter value rather any feed back value

- must have diff key and Counter value for every plaintext block (never reused) again.

Q2 a). Create a object called cipher in Cipher class with using AES encryption method using CBC with PKCS5 padding.

(b).

user A generate cipher text

$$C = E_{K2}\Big[\underbrace{D_{K1}\big[\underbrace{E_{K1}[P]}_{\text{encrypt plaintext using k1 key}}\big]}_{\text{decrypt ciphertext using k1 key.}}\Big]$$

k1, k2 Symmetric key

now $\underbrace{C = E_{K2}[P]}_{\text{Encrypt plaintext using K2 key.}}$

Date:.............................

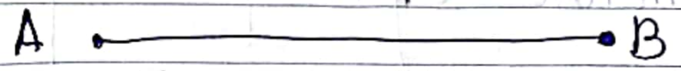
$$P = DK2\underbrace{[EK3\underbrace{[DK3[C]]}_{\text{Decrypt ciphertext using K3 Key}}]}_{\text{Encrypt plaintext using K3 key}}$$

K2, K3 Symmetric key

$$P = D\underbrace{K_2[C]}$$

* decrypt ciphertext using K2 key

(C) (i)



public key B = (27, 55)
private key A = (3, 55)

(i) A message M=10 send to B

Signature S of message M

$$S = 10^3 \bmod 55$$

Signature = 10 S=10

(ii) A message M=13 Signature S = S=10

Cipher text message $13^{27} \bmod 55$
$= 7$

Signature $= 13^3 \bmod 55$
$= 52$

Date:..........................

(d) pkcs7 signed data - signed and authenticate
pkcs7 Envelop data - encrypt and confidentiality
pkcs7 signed data & envelop data
- above both.

03 (a)

(i) * need secure method to exchange secret key
* choices are RSA or Diffie-Hellman

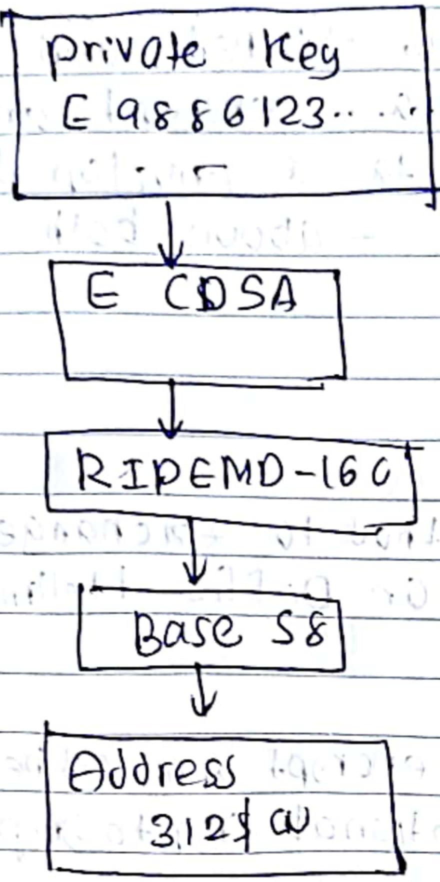
* "Key pair" used
(either one can encrypt and other can decrypt)
* slower than conventional cryptography

(ii) * higher latency compared to other encryption protocols
* older TLS version vulnerable to MIM attacks
* Few platforms support TLS 1.3

(iii) Diffie Hellman

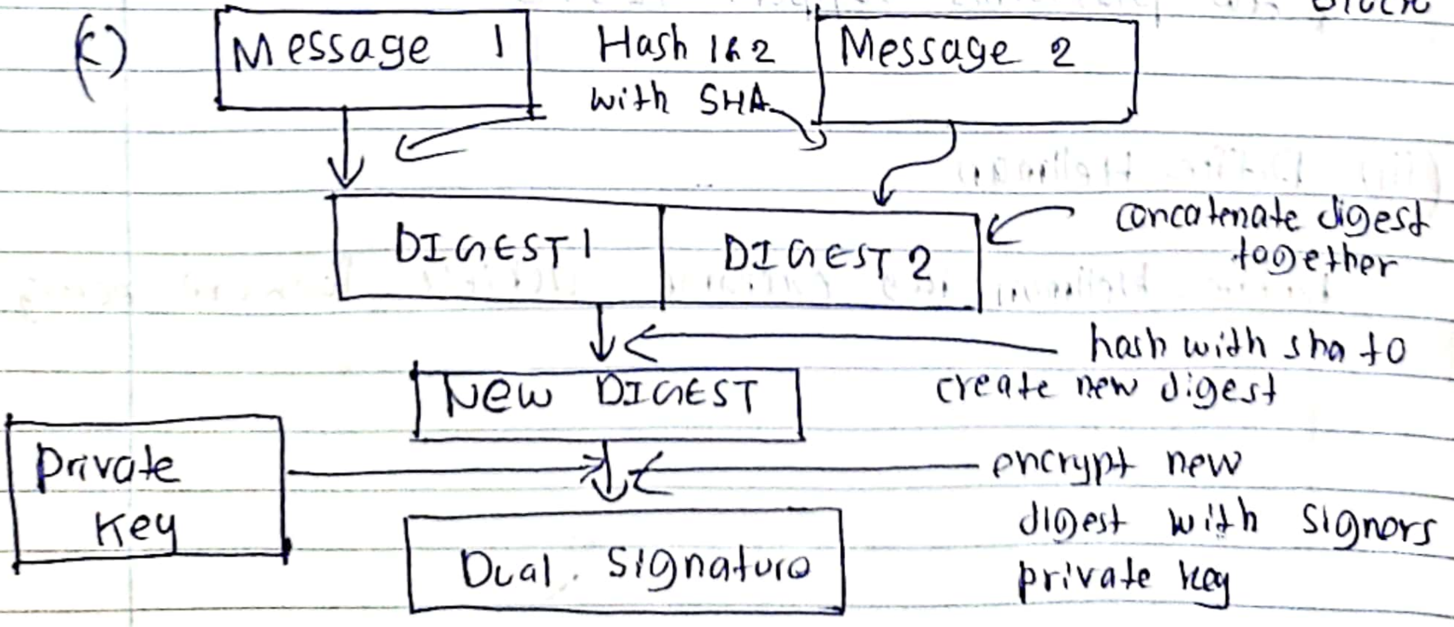
Diffie Hellman key exchange achieve forward secrecy

(b) (i)



(ii) process of turning transaction into blocks.
New Correncg Created by rewarding miner
miners venify transaction, it turns into transaction block

(c)



concatenate digest together

hash with sha to create new digest

encrypt new digest with signors private key

Date:..............................

04 (a)

(b)

(C). idintify and classify sensitive data
use data encryption
harden your Systems
Allocate roles

(d) Because username have lower entrophy than a random Salt