Information System Security

SCS 2214 [2021]

01 (a).

Attack

* A human exploitation of vulnerability

Vulnerability

* weakness in the security system

Control

* protective measure
* An action/device or measure taken that removes, reduces or neutralizes a vulnerability

Problems

* Consequences of unintentional accidental errors

thread

* A set of circumstances that has the potential to cause loss or harm

Risks

* Probabilities that same threat or problem will occur due to system vulnerabilities

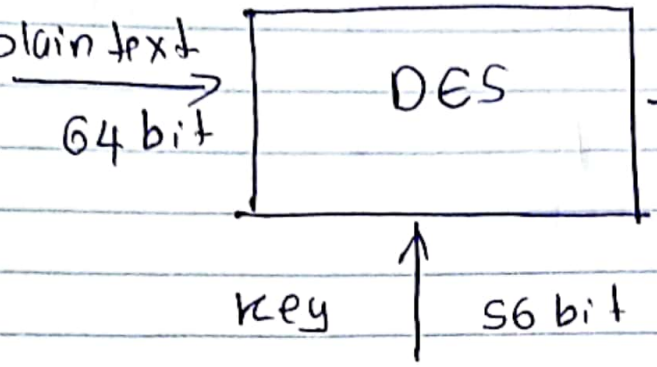
(b) 1. Encryption
2 SW & HW Controls
3. policies
4. physical controls

(c)

plain Text :	V	E	R	N	A	M	C	I	P	H	E	R	
Numeric Equivalent :	21	4	17	13	0	12	2	8	15	7	4	17	
+ random Numbers :	76	48	16	82	44	3	58	11	60	5	48	88	
= Sum :	97	52	33	95	44	15	60	19	75	12	52	105	
= Mod 26 :	19	0	7	17	18	15	8	19	23	12	0	1	
Cipher Text :	t	a	h	r	S	p	I	t	X	m	a	b	

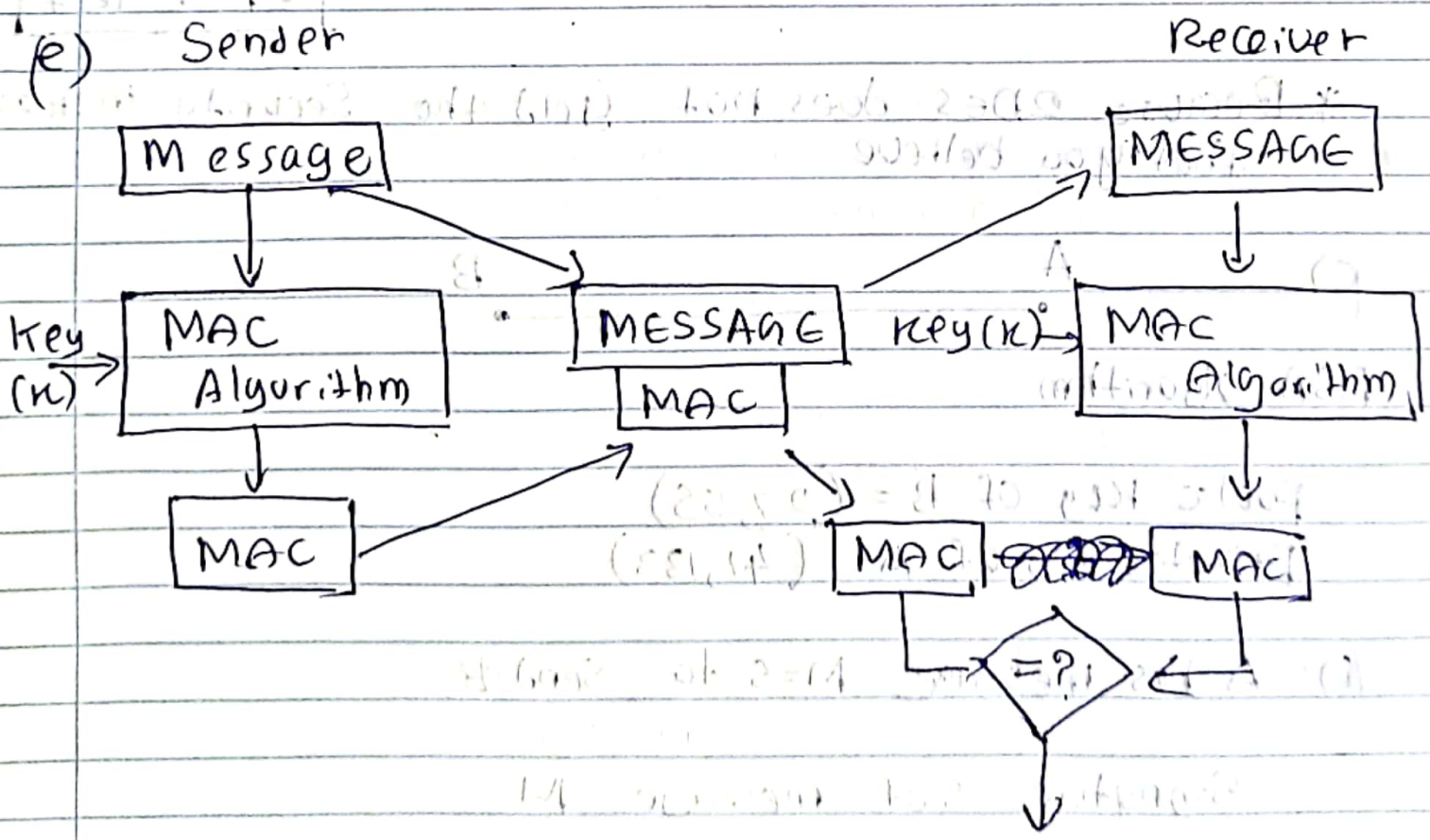
* Cipher text bears no Statistical relationship to the plain text Since for any plain text & any Cipher text there exist key mapping one to other.

(d)



Block Size = 64 bits
key Size = 56 bits. (really 64 bits, but 8 are used as parity check bit for error control)
no! of rounds = 16
16 intermediary keys, each 48 bits.

(e)



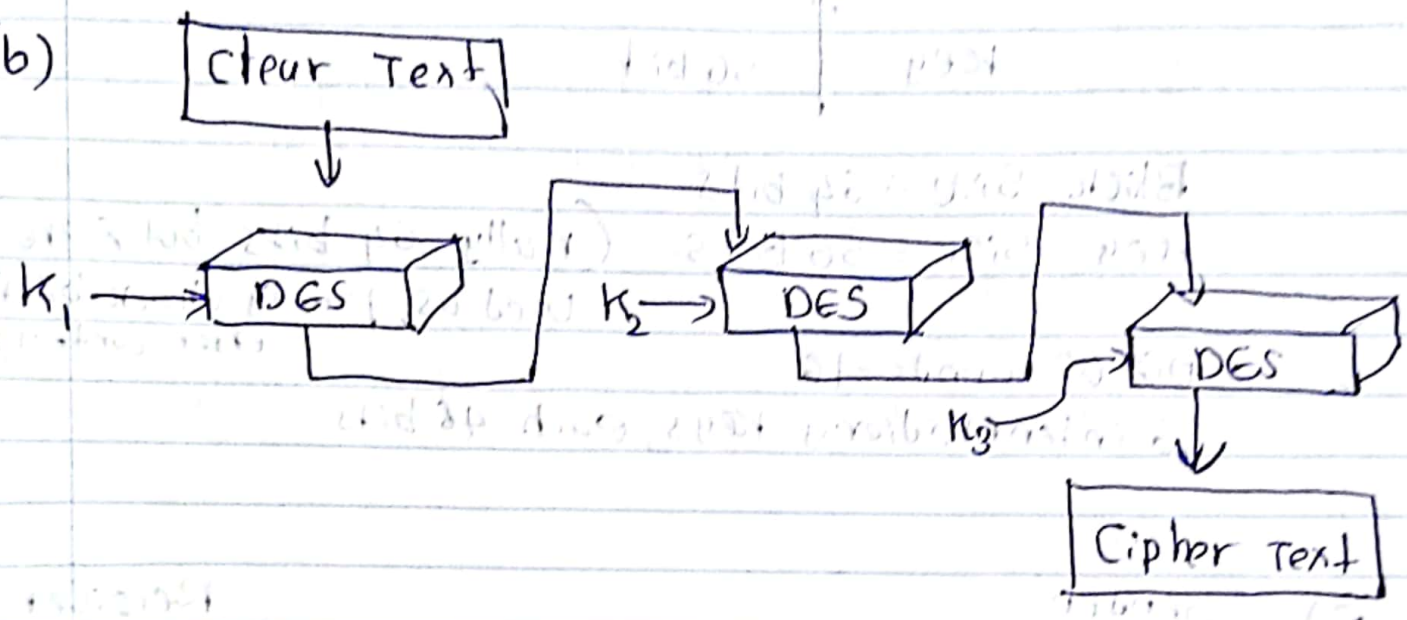
if Same, MAC found, then message is authentic

Q2 (a)

(i)

(ii)

(b)



* Because 2DES does not yeld the Security increay that you believe

(c)

RSA olgorithm

Public Key of B = (27, 55)
Private key of A = (41, 133)

(i) A has message M = 5 to Send B

Signature S of message M

$S = 5^{41} \bmod 133$

$S = 66$

Date:.....

(ii) A encrypt message M=10

$S = 10^{41} \bmod 133$

$S = 117$

$C = 10^{27} \bmod 55$

Cipher text = 10

03 (a) (i). Mac fasten than digital signature.
Mac are easy to use.

(ii). public key infrastructure (PKI)

* provide fandation necessary for secure e-business through use cryptographic keys and certificates.

(b)

Signature

No:.....

Q4 (a)

* Vpn connection established secure connection you and the internet

* Using vpn all data traffic is routed through an encrypted virtual tunnel

* this disguise your ip address when you use internet
* Making its location invisible to everyone
* ⊖ vpn connection is also secure against external attacks

(b)

(c) Can detect attacks that cannot seen by NIBIDS since they monitor events local to a host

Unaffected by switched networks

Can operate where network traffic is encrypted

(d) Firewall
Malware detection
Vpn capabilities
routing capabilities

Date:

e). Yes

Storing salt in another table not really add any significant security