CS 478 Midterm

Q.1 (30pts.) (no justification needed)

1) False. Encryption only provides confidentiality, not integrity.

2) True. DoS & DDoS both target availability.

3) True. Kerckhoff's principle.

4) False. Shift-by-n only needs 26 tries for brute-force attack (keyspace = 26)

5) False. We don't use F^{-1} anywhere in DES.

6) False. What's given is the defn. of confusion.

7) True.

8) True

9) No. AES is based on S-P network, not Feistel.

10) True.

11) True.

12) True. e.g; AES has 10/12/14 rounds.

13) False. Min. requirement is security against CPA attacks.

14) False. Digital certificates are signed by TTPs, not encrypted.

15) No. Public-key encryption doesn't provide non-rep. Only public-key signatures do.

Q.2 (9 pts)

a) DES is a shared key cryptosystem. (+1)
Key length is too small - only 56 bits,
So it is insecure. (+2)

b) 3DES adds 2 layers of encryption
& 1 layer of decryption, e.g.,

$$C = E_{K_3}\left(D_{K_2}\left(E_{K_1}(M)\right)\right), \quad (+1)$$

So effective key length is 168-bits
(or 112-bits if you set $K_1 = K_3$). (+2)
Much larger key length than plain DES.

c No. 2DES is vulnerable to (+1)

Man-in-middle attack. Attacker needs a (P, C) pair, then builds a table*.

[$C = E_{K_2}(E_{K_1}(P))$]

P	C
$E_{K_1^1}(P) = X_1$	$D_{K_2^1}(C) = X_1'$
$E_{K_1^2}(P) = X_2$	$D_{K_2^2}(C) = X_2'$
⋮	⋮
$E_{K_1^{2^{56}}}(P) = X_{2^{56}}$	$D_{K_2^{2^{56}}}(C) = X_{2^{56}}'$

At some row, there will be a match in the 2 columns of the table - since each key, K_1, K_2 can have only 2^{56} value each.

(+2)

Q.3 (10 pts.)

Possible values of X, Y, Z registers' majority bit: (000, 001, 010, 011, 100, 101, 110, 111)

a) Pr [X, Y, Z all stepping] = 2/8 = 0.25

b) Pr [X and Z step] = 4/8 = 0.5

(hard to assign partial credit!)

Q.4 (35 pts)

a) (7 pts) |P| = 9173 bits, block length = 256 bits

9173 = 256 * 35 + 213, 256 * 36 = 9216

So we have 36 blocks of plaintext & ciphertext. (+5)

(+2)

Size of IV = size of first block = 256 bits

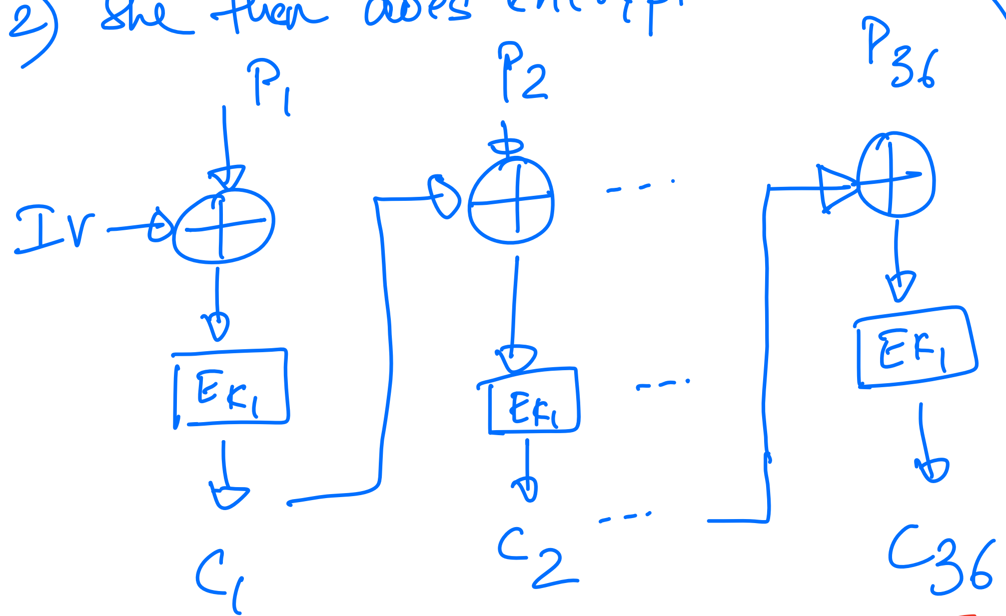
(14 pts) (Alice's side)

Alice   Bob

1) Alice generates (+2)
IV, s.t. |IV| = 256 bits, and generates K_1; $|K_1| = 128$ bits

Different keys for enc. & MAC

2) She then does encryption:

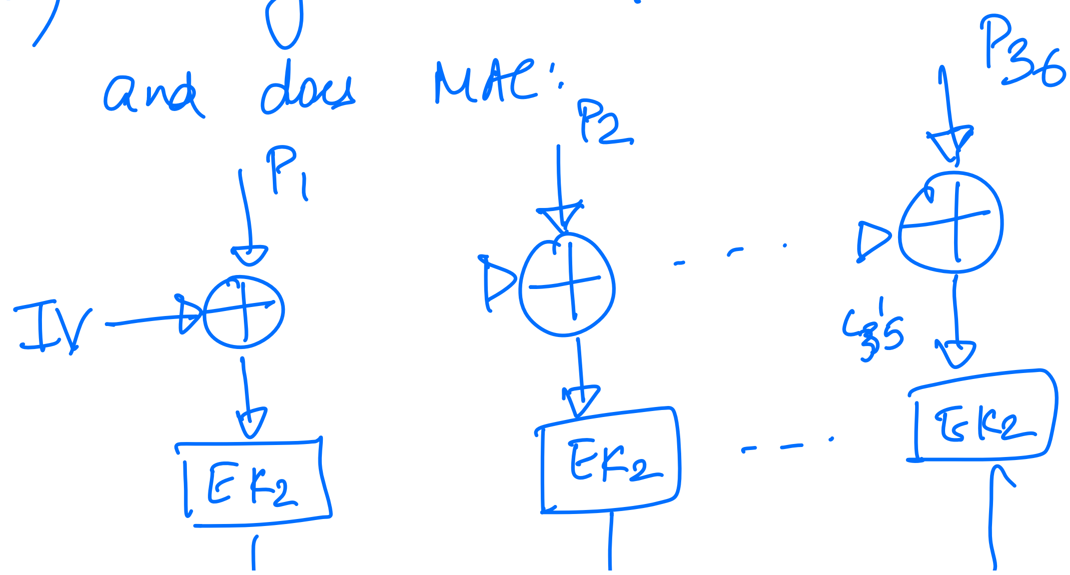


(+4)

Can't be general, e.g., "Cn"

3) She generates key K_2; $|K_2| = 128$ bits,

and does MAC:



$K_2 \neq K_1$

(+4)

$\downarrow$ $\quad\quad$ $\downarrow$ $\quad\quad$ $\downarrow$

c_1' $\quad\quad$ c_2' $\quad$ - - $\quad$ $\boxed{c_{36}' = MAC_A}$

4) Alice sends to Bob:

a) $c_1, c_2, \ldots, c_{36}$
b) IV
c) MACA

could be sent through insecure channels.

(+4)

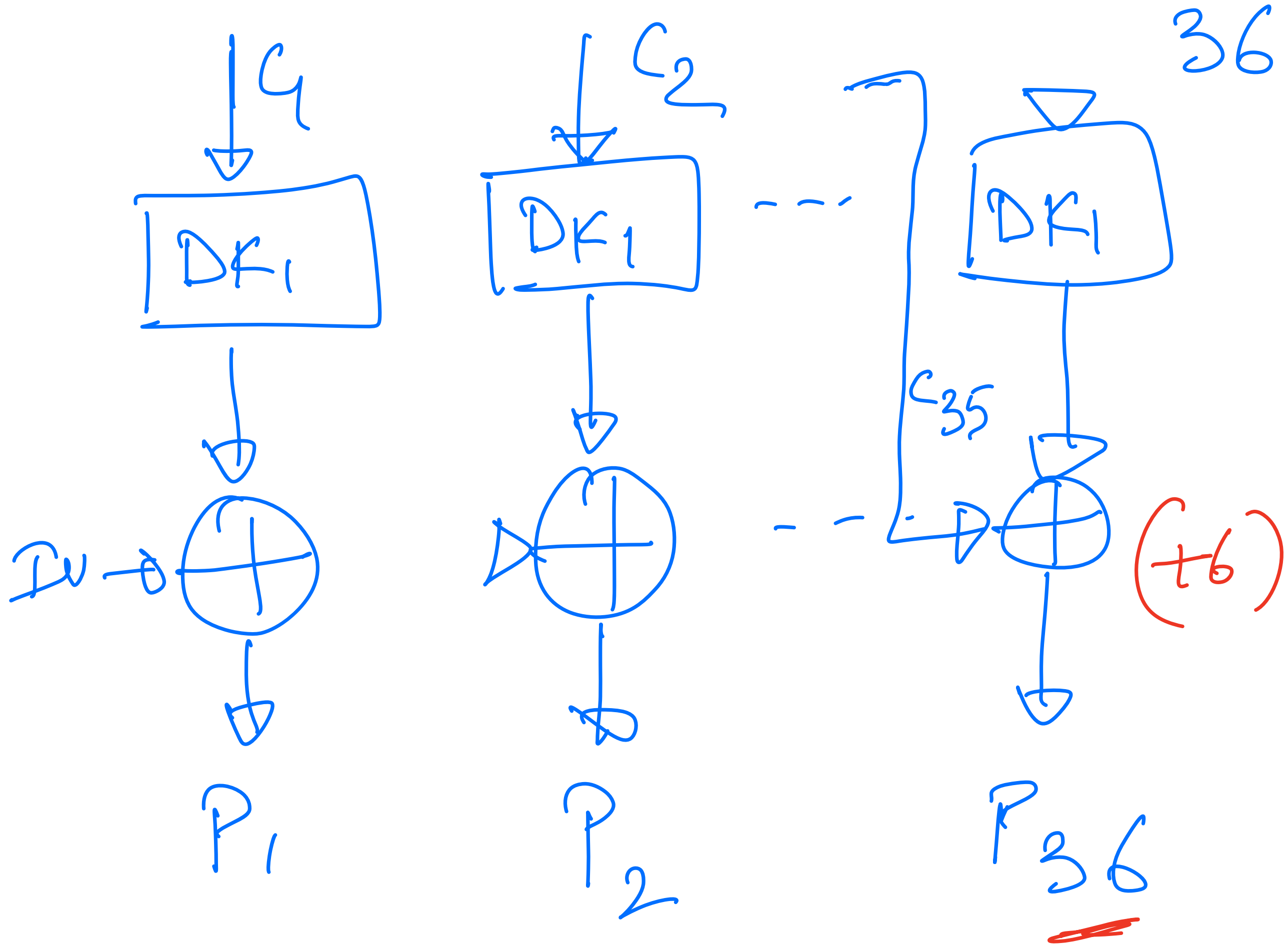
d) K_1 & K_2 (through a secure & authenticated channel)

(14 pts) Bob's side

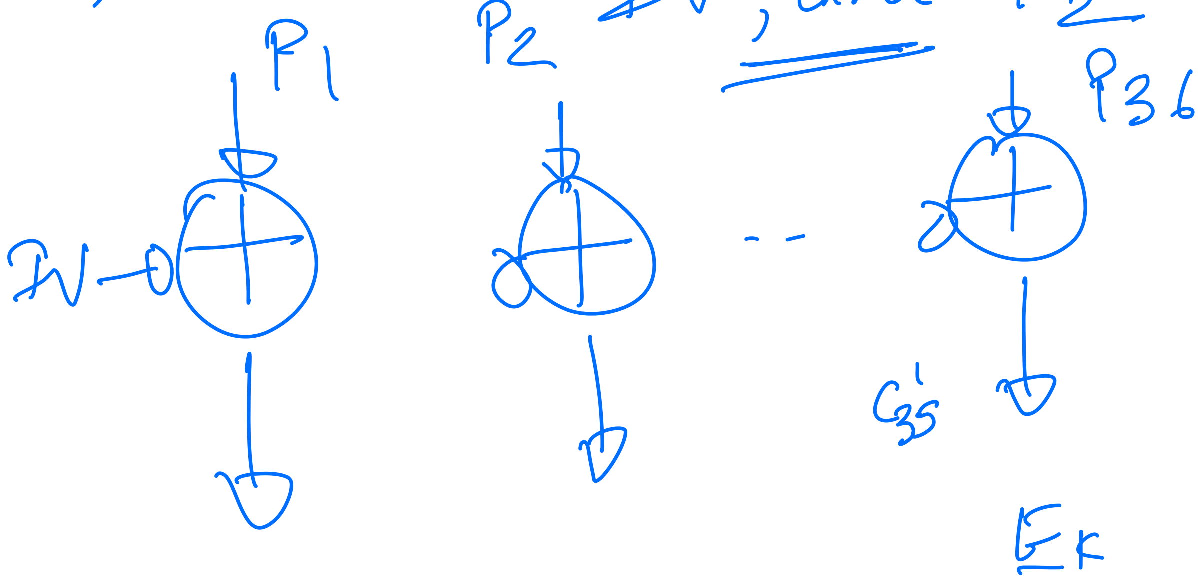
Bob

5) Bob receives (a, b, c, d) from Alice in step 4.

6) Bob does decryption:



7) Bob verifies MAC w/ ($P_1, \dots P_{36}$) IV, and K_2



E_{K_2} $\quad$ E_{K_2} $\cdots$

$\downarrow$ $\quad$ $\downarrow$ $\quad$ $\downarrow$

C_1' $\quad$ C_2' $\cdots$ $\quad$ $\boxed{C_{36}' = MAC_B}$

$(K_1 \neq K_2)$ $\quad$ $(+6)$

8) If $MAC_B = MAC_A$, BOD accepts, else rejects MAC_A. $(+2)$

Q 5. a) (8 pts)

Alice does:

$C_1 = E_K(ctr+1) \oplus P_1$

$$C_2 = E_K(ctr+2) \oplus P_2$$

$$C_3 = E_K(ctr+3) \oplus P_3$$

$$\vdots \qquad \vdots \qquad \vdots \quad \vdots$$

$$C_n = E_K(ctr+n) \oplus P_n$$

Say Trudy changes C_1 to X,

$$P_1 = X \oplus E_K(ctr+1)$$

↳ incorrect

$$P_2 = C_2 \oplus E_K(ctr+2)$$

↳ correct

rest of decryptions P_1 is not

involved

So if C_k is changed to X, (+8)

Only P_k will be decrypted

incorrectly. Rest will be fine.

b) (8pts)

Trudy changes ctr to ctr'

$$P_1 = C_1 \oplus E_K(ctr' + 1)$$

↳ incorrect

$$P_2 = C_2 \oplus E_K(ctr' + 2)$$

↳ incorrect

Rest will also be incorrect.

So all blocks will be decrypted incorrectly. (+8)