Your name: _____, Roll no.: _____

CSE 350/550: Network Security, Mid-semester exam: Feb 29, 2024, 90 minutes, 90 marks

Instructions:

- The exam is in **two** parts: Part 1 has 8 questions that require short answers. Each question is for 5 marks ➔ 40 marks. Part 2 has 5 questions that require longer answers. Each question is of 10 marks ➔ 50 marks.
- This is a "closed-book" exam. All necessary information, including tables, etc. will be provided here.
- Write your answers in the space provided. If necessary, use a separate sheet for rough work.
- Do not use unfair means. Action will be taken against you if you use unfair means. You may not use books, notes, computer, smart phone, etc. or share info with other students. You may only use a calculator.

Part 1: 8 questions that require short answers (5 marks each)

1. Using an ideal substitution cipher with 5-bit input and 5-bit output:
   a. what is the size of the table that maps an input to its output? (1) $32 = 2^5$
   b. what is the potential number of keys that help construct the table? (2) $32!$
   c. what is the key size in bits - simply state the formula to compute this? (2) $\log_2(32!)$

2. Assume we are using a linear congruential PRNG to generate a byte stream: X(n+1) = a * X(n) mod m, with m = 11, a = 4, and X(0) = 5 for instance. What is the periodicity of this PRNG generator? Hint: go ahead and compute the sequence of random numbers generated, with the initial X(0) = 5. Show your working here.

(4) $X(0) = 5$, $X(1) = 20 \bmod 11 = 9$, $X(2) = 36 \bmod 11 = 3$, $X(3) = 12 \bmod 11 = 1$, $m(4) = 4$, $X(5) = 16 \bmod 11 = 5$
➔ periodicity 5 ← (1)

3. It is known *Triple* DES with 2 keys is significantly stronger when compared to *Single* DES. What is that fundamental property of DES that allows this to be the case? State your answer briefly.

(2) There does not exist K s.t. $DES(DES(X, K1), K2) = DES(X, K)$ for all X, K1, K2. Thus
(2) Two stages of DES cannot be reduced to one stage of DES.
➔ ~~Three stages~~ Triple DES cannot be reduced to single DES. (1)

4. Consider an RSA based public key cryptosystem, where n = 55. The public key e = {9, 55} is used to encrypt a message resulting in ciphertext C = 4. Can an intruder determine the message, M? If so, what is M? Show details of your working.

(2) Step 1: factor $n = 55$ as $n = 55 = p * q = 11 * 5$.
(1) Step 2: $\Phi = (p-1)(q-1) = 40$
(1) Step 3: given $e = 9$ compute $d = 9$ since $e * d = 81 \bmod 40 = 1$
(1) Step 4: $M = C^9 \bmod 55 = 4^9 \bmod 55 = 14$

5. What makes the RSA based cryptographic scheme so difficult to crack? That is, what is that fundamental property involving publicly known parameter n, and public (encryption) key, (e, n), that makes it near-impossible for one to discover the private key, (d, n)?

(3) Given knowledge of (e, n) it is ~~not poss~~ nearly impossible to ~~factor n to obtain p*q = n~~ and thus obtain Φ,
(2) (1) compute d such that $e * d \bmod \Phi = 1$ since Φ is not known.

6. It is understood that distribution of 'Public keys' in a Public-Key Cryptosystem should be done in a secure manner. Why is that? Answer the question in the context where message M is to be transferred from A to B in a confidential manner after encrypting it. Note: public key (e, n) is used to encrypt while private key (d, n) is used to decrypt. In other words, what would be the undesired consequence if the public key was compromised?

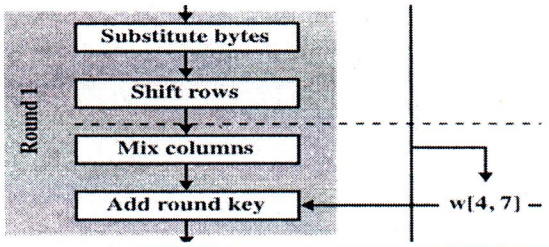
(5) Sender uses public key (e,n) of receiver to encrypt message M. If he uses a wrong/fake public key (say (e2,n)) of receiver then the individual who has the dec key (d2,n) corresponding to (e2,n) will be able to decipher the cipher text. ⇒ It is IMP for sender to use correct (e,n)

7. Consider symmetric key cryptography. In order to establish a shared key for a new session, parties A and B must already have established a 'master session' between themselves. Why is there a need to set up a new session given that a 'master session' already exists?

(2) Master keys are used sparingly only to establish session keys.
(3) Alternatively if master key is used to exchange all messages, it is likely to be compromised.

8. Consider AES. A portion of the input to 'Substitute Bytes' of the kth round is given below. What is the last row of the output from 'Substitute Box' and similarly from 'Shift Rows'? The S-box table is given below:

-	-	-	-
-	-	-	-
-	-	-	-
AC	40	52	B2



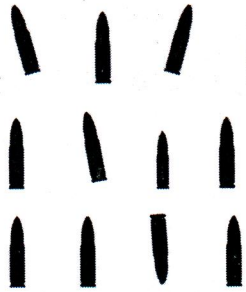
x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Output of 'Substitute Box': 91 09 00 37 ← (2)

Output of 'Shift Rows': 37 91 09 00 ← (3)

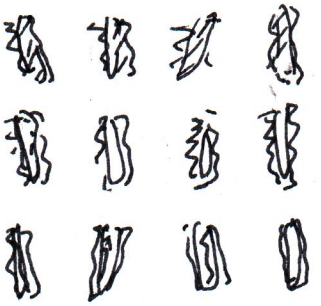
Part 2: 5 questions that require relatively long answers (10 marks each)

9. I have a Black-and-White photo (with no grayscale) of size 1024 x 1024 pixels of bullets seized from a suspected terror attack, all laid out neatly on a white table top. See below for an example image.



I wish to communicate this image (of 1024 x 1024 pixels) to district headquarters using DES encryption. Assume that each pixel is encoded using 8 bits. And each block of 8 pixels in a given row is encrypted using DES. This results in an encrypted image consisting of 1024 x 128 array of 64-bit ciphertexts which can possibly be displayed as 1024 x 1024 pixels (now possibly with greyscale) before or after decryption.

a. Sketch what the photograph may look like AFTER it is encrypted.



6

① the grey scales inside the image of bullet and those outside will be very different

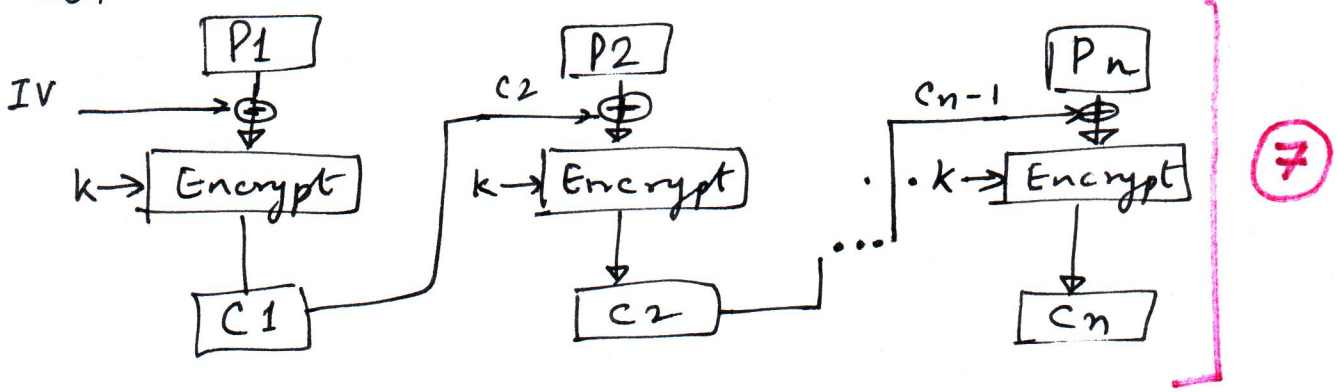
② the edges will be significantly blurred.

b. Is it at all possible for an intruder to look at the encrypted image and estimate the number of bullets seized from the attack? Explain why that is possible or not possible.

4 Yes, as explained above the grey scales inside & outside the image of a bullet will be very different, while the edges are very much blurred.

10. Continuing with Question 9, if you were to encrypt the photograph differently, how would you encrypt the blocks of eight pixels so that it is NOT possible to determine the number of bullets seized? Draw one or more diagrams to illustrate your solution.

3 Use block chaining. See below, where "initial value" IV is held secret. K is the key. P1, P2, Pn are, for example, 64 bit blocks.



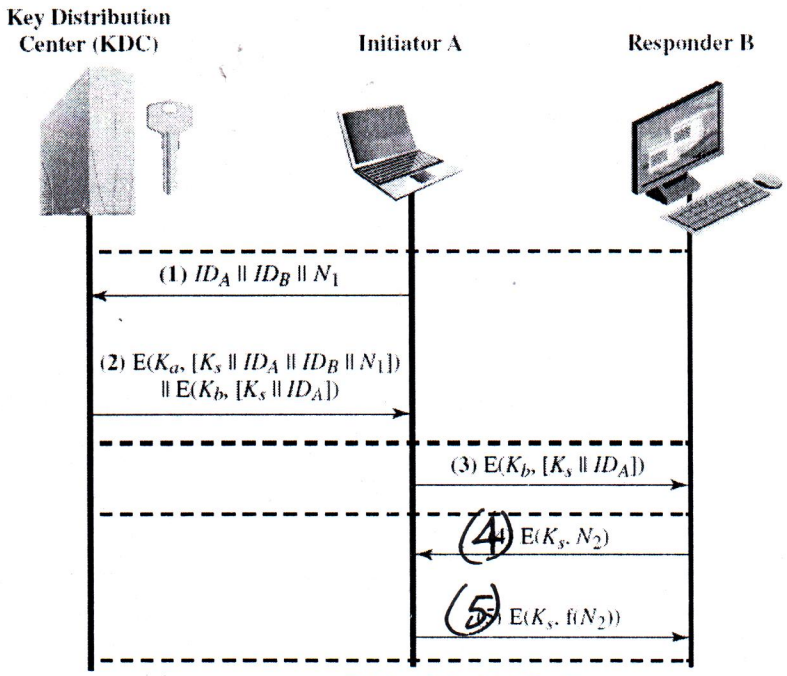
7

11. Consider RSA based cryptosystem, with p=17, q=7, encryption key e=13. Use extended GCD algorithm (or table below) to compute decryption key, d. Show your working below in form of values of Q(i), R(i), S(i), T(i), with i=2, 3, etc.

	Quotient, Q(i)	Remainder, R(i) R(i+1) = R(i-1) - Q(i+1)R(i)	S(i) S(i+1) = S(i-1) - Q(i+1)S(i)	T(i) T(i+1) = T(i-1) - Q(i+1)T(i)
0		Φ=~~7~~ 96	1	0
1		e =~~7~~ 13	0	1
2	~~7~~ 7	~~7~~ 5	~~7~~ 1	~~7~~ -7
3	2	3	-2	15
4	1	2	3	-22
5	1	1	-5	37
6, etc.				

What is the decryption key, d = 37

12. One way devices A and B can share a symmetric encryption key, K_s, is to obtain the key from a "key distribution center", KDC, using an existing secure channel between A and KDC, & between B and KDC (as given below).



A. Above, why does KDC include $E(K_b, [K_s \| ID_A])$ within message numbered (2) sent to Initiator A, and not send directly to responder B? In other words, how does it help?

Optimize its workload by reducing the no. of message it has to send.

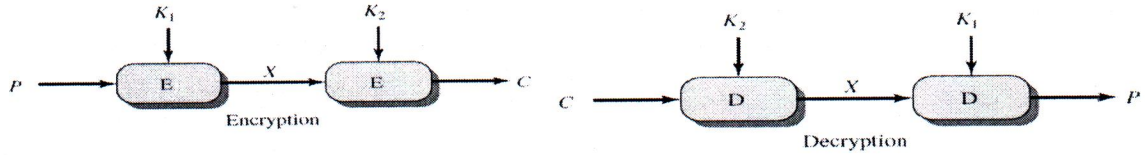
B. What purpose do messages numbered (4) and (5) serve?

Confirm that both A & B are able to use the same session key K_s, and the session has bee established

C. In message (5) could $f(N_2)$ be replaced simply by N2? Explain briefly.

NO. Since an intruder can simply copy the entire ~~message (sent by B to A)~~ and send it back to B, thus claiming itself to be initiator A without gaining any benefit, ~~except~~ possibly prevent A & B from communicating.

13. Consider using 2 stages of DES. That is, given 64-bit plain text P, the ciphertext $C = E_{K2}(E_{K1}(P))$ where key K_1 is used in stage 1, and key K_2 is used in stage 2, as given below.



Argue as to why time complexity of a brute-force attack on 2-stage DES is nearly the same as that for 1-stage DES. To do so:

a. Describe how a brute-force attack on 2-stage DES may be launched.

ASSUMPTION: Intruder has access to ~~at least~~ one or more pair(s) (P, C).

Step 1. For a given (P, C)
(a) compute $X_{K1} = E_{X1}(P)$ for all possible X1
(b) compute $Y_{K2} = D_{X2}(C)$ for all possibe X2
(c) Sort the set of X_{K1}
(d) Sort the set of Y_{K2}
(e) Determine K1 & K2 s.t. $X_{K1} = Y_{K2}$

(4)

Step 2 Repeat step 1 with different set (P, C) & confirm if the same K1 and K2 yield $X_{K1} = Y_{K2}$.

(2)

b. What would be the time complexity of the attack described in a. above.

$O(2^{56}) + O(2^{56}) + 2^{56}\log(2^{56}) = O(2^{56})$

(2)

c. Whether the attack described in a. above will absolutely positively determine the keys K_1 and key K_2? Or many such attacks described in a. above would be necessary to increase one's confidence in the keys K_1 and key K_2 So discovered?

Above step 1 (only) is not enough. We need to check in step 2 with other pairs of (P, C) so that the level of confidence in determining K1 & K2 is increased.

(2)