Name: _____, Roll No.: _____

CSE 350/550: Network Security
Quiz 1: TUE Feb 13, 2024

Instructions:

- There are 5 questions, each 6 marks, for a total of 30 marks. Total time available 30 minutes.
- Provide answers in the space provided only. You may do your rough work on a separate blank sheet.
- You may use a calculator, but nothing else. **Pl. keep your phones/laptops, books etc. away from you**.
- Do not use unfair means, else action will be taken. Do not use material such as books, notes, etc. or a computer, smart phone, etc. And do not share information with other students.

1. Consider a crypto-system similar to Caesar-cipher, but where c=p*k mod 26. Here the set of symbols is {0, 1, 2, ..., 24, 25}, p is plaintext, c is ciphertext, k is key. For example, if key=3, p=15, then c=19. Is there a constraint on the value of key, k? If so, what condition must k satisfy to qualify as a valid key. BE BRIEF.

6 marks

k must be such that (26, k) are co-prime. In other words, 26 and k do not have a common factor. To be sure the factors of 26 are 2, 13. Thus k should NOT have 2 or 13 as a factor. Examples of k that are allowed are are: 3, 5, 7, 9, 11, 15, 17, 19, 21, 23. the rest is some explanation

2. Consider a transposition based cryptosystem discussed in class, where the key is [6; 3 2 1 4 5 6]. If the ciphertext is LUANIDYEDENAWLLGALEELAJX then what is the plaintext?

6 marks

DILWALEDULLANYALEJAENGEX

3	2	1	4	5	6
D	I	L	W	A	L
E	D	U	L	L	A
N	Y	A	L	E	J
A	E	N	G	E	X

this is how one could have gotten the answer

3. An S box in DES is a 6-bit input, 4-bit output substitution box (given below). The table therein used in Round 1 is also given below.

(a) What is the resulting output when input is **011110**?

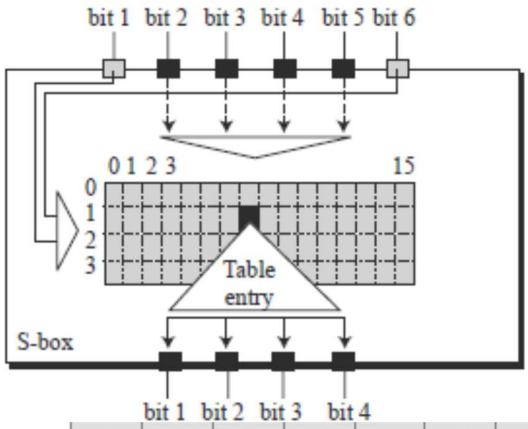
3 marks

07, or 0111

(b) What is the resulting output when input is **110011**?

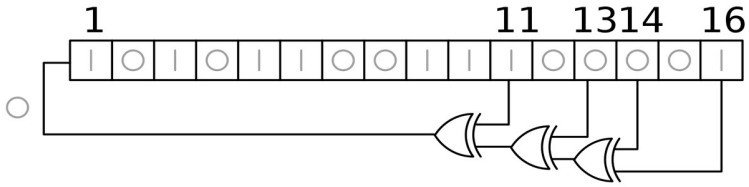
3 marks

11, or 1011



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

4. Consider the operation of a pseudo-random number generator based on a 16-bit linear feedback shift register shown below. What are first TWO 16-bit random numbers generated following 1010 1100 1110 0001 or 'ACE1' in Hexadecimal digits? Bit 1 is most significant, while bit 16 is least significant. Write these as Hexadecimal digits.



2 marks

5670
AB38

4 marks

5. Consider AES, and the substitution box in an encryption round. This S-box is given below in form of a table. What is the output of the S-box if the input byte is (hexadecimal) 25. FURTHER, as part of decryption one has to do an INVERSE S-box substitution. However, I do not know what that INVERSE S-box table is. But can you figure out as to what would be the output of the INVERSE S-box if the input is FA?

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	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

2 marks

S-box substitution during encryption of Hexadecimal 25: S(25) → 3F

INVERSE S-box substitution during decryption of Hexadecimal FA: Inverse-F(FA) → 14

4 marks