Department of Computer Science and Engineering
Indian Institute of Technology Bhilai
CS553/CSL505 – **CRYPTOGRAPHY**

Mid-Semester Exam
September 27, 2024

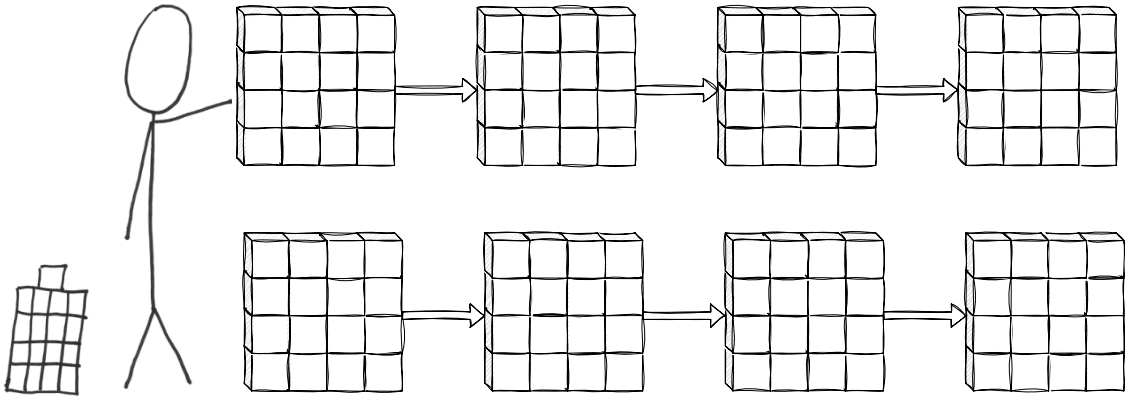
Student's Name Roll No.

Time: 3 hours Maximum Marks: 90

1. (a) Recall the following statement from the Stick-Figure Guide to AES. $(5_{/10})$

> If you look carefully, you'll see that each bit of a round's output depends on every bit from two rounds ago.

Justify the statement pictorially in the light of two rounds of AES *decryption* using the state diagram below. Label the edges to show the round sub-operations. You may ignore the And-Round-Key sub-operation.



(b) State the theorem related to one of the AES sub-operations that you used in Part a. $(3_{/10})$

(c) What was the statement given in Part a used to decide in the design of AES? $(2_{/10})$

2. (a) Differentiate between affine and linear functions. Give examples of both. $(4_{/10})$

(b) There is only a single coordinate required to draw a linear function. Justify. $(2_{/10})$

(c) Using your answer to Part a, justify why the Affine Cipher is named so? $(2_{/10})$

(d) Name the component of AES round function that involves an affine transformation in its generation. $(1_{/10})$

(e) Which attack model is the Affine Cipher vulnerable to? $(1_{/10})$

3. (a) While using OTP scheme, Alice sees that if $k = 0^n$, then $e_k(m) = m$ meaning that the plaintext is sent as it is. To stop, this she decides not to use $k = 0^n$ implying that keys are now uniformly chosen from $\{0,1\}^n \setminus 0^n$. What is the effect on perfect secrecy due to this decision? ($5_{/10}$)

(b) Alice wishes to regularly send Bob a plaintext message P_1 or P_2. On each occasion she chooses to send either P_1 or P_2, but on average she chooses the plaintext P_1 twice as often as she chooses the plaintext P_2. Each time, Alice uses a (very simple) symmetric cryptosystem, with the same fixed key K, to encrypt the plaintext. When she chooses P_1, the ciphertext is $C_1 = E_K(P_1)$; when she chooses P_2, the ciphertext is $C_2 = E_K(P_2)$. Suppose an attacker knows the only possible plaintext messages are P_1 and P_2.

i. Suppose the attacker does not know Alice chooses P_1 twice as often as P_2. What observation will the attacker, who can only see the ciphertexts sent from Alice to Bob, make? ($3_{/10}$)

ii. Suppose the attacker learns Alice chooses P_1 twice as often as she chooses P_2. What does the attacker now learn? ($2_{/10}$)

4. Compute the following:

   (a) $\log_{x \oplus 1}(x^3 \oplus x^2 \oplus x \oplus 1)$ $(2_{/10})$

   (b) Multiplicative inverse of 5 in $\mathbb{Z}_{12}$? $(2_{/10})$

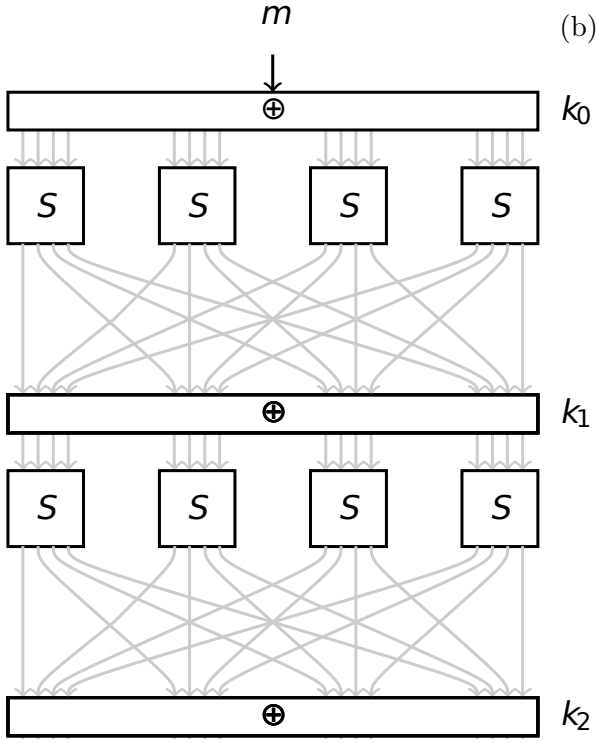
   (c) $\frac{1}{5} \bmod 11$ $(2_{/10})$

   (d) Number of different substitution ciphers for binary words of length n $(2_{/10})$

   (e) The size of the key-space of the Vigenre cipher with a keyword of length 13 $(2_{/10})$

5. (a) Consider the following DDT you saw in class. Find a characteristic such that total number of active SBox-es is ***exactly*** 6. Highlight it in the figure (use a **pencil** if needed). Show the step-by-step computation of its probability? ($5_{/20}$)

in \out	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2



(b) Probability Calculation: ($3_{/20}$)

(c) Define differential uniformity (DU)? What is the DU of the SBox corresponding to the DDT given above? State the transition that leads to it. ($4_{/20}$)

(d) What is an impossible differential transition? Give an example referring to the DDT give above. ($2_{/20}$)

(e) Briefly explain the idea of filtering. ($3_{/20}$)

(f) What is the filtering criteria for the characteristic you reported in the last question considering this as a 3−round cipher? ($3_{/20}$)

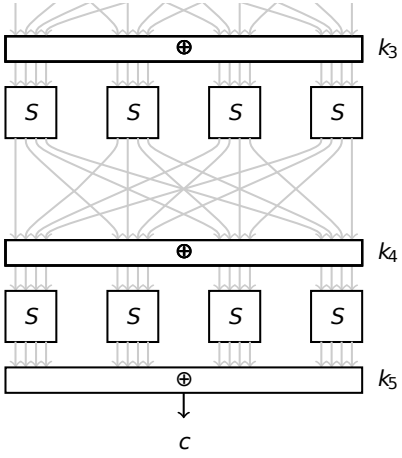
(g) What does the value of an entry in the Linear Approximation Table (LAT) signify? [3 (bonus)]

(h) If a Simple Substitution Cipher is used (with an unknown key) and we intercept the ciphertext `OXAO`, then which of the following four-letter words could be the plaintext: `JOHN, SKID, SPAS, LOOT, PLOP`, or `OSLO`? [2 (bonus)]

6. Recall the last round of Sypher004

   (a) With proper mathematical arguments state why adding the permutation layer in the last round would *not* have improved the security of Sypher004. ($6_{/10}$)

   Use the following notations: $P \rightarrow$ permutation, $t \rightarrow$ intermediate state value after last round SBox layer.



   (b) What is the hardware implementation perspective on the above design decision. ($4_{/10}$)

7. Answer in brief.

   (a) Explain why it is reasonable to claim that a one-time pad is immune to an exhaustive key search. ($2_{/12}$)

   (b) What is meant by a generic attack? Compare the (D, T, M) of the Brute-force and Codebook attacks. ($3_{/12}$)

   (c) What is meant by security-margin of a block-cipher? State the security-margin of AES. [3 (bonus)]

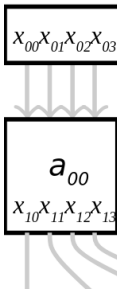
   (d) Arrange the following in terms of increasing power of the attacker: CCA, COA, Ad-CPA, KPA, Ad-CCA, CPA. ($2_{/12}$)

 Question 7 continues on the next page...

(e) For typical values of block-size n, and key-size k, a block cipher provides only a tiny fraction of all the available permutations. Explain this in terms of the Shift Cipher and then in terms of Sypher004. $(5_{/12})$

8. (a) The MILP model made in class for Sypher004 was incomplete. Justify. $(3_{/8})$

(b) What is the problem with the following constraint? Explain with the help of a transition. $(3_{/8})$



$$4x_{10} + 4x_{11} + 3x_{12} + 4x_{13} - (x_{00} + x_{01} + x_{02} + x_{03}) \geq 0$$
$$4x_{00} + 4x_{01} + 4x_{02} + 4x_{03} - (x_{10} + x_{11} + x_{12} + x_{13}) \geq 0$$

 Question 8 continues on the next page...

(c) Now generalize the above constraint for an $n-$bit SBox. $(2_{/8})$

(d) What is probability of the differential characteristic for 3 rounds of AES discussed in class? 2 (bonus)
What is the same for an equivalent random transformation?
