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

Mid-Semester Exam
October 3, 2023

Time: 120 mins | Maximum Marks: $10 \times 4 + 15 \times 4 = 100$

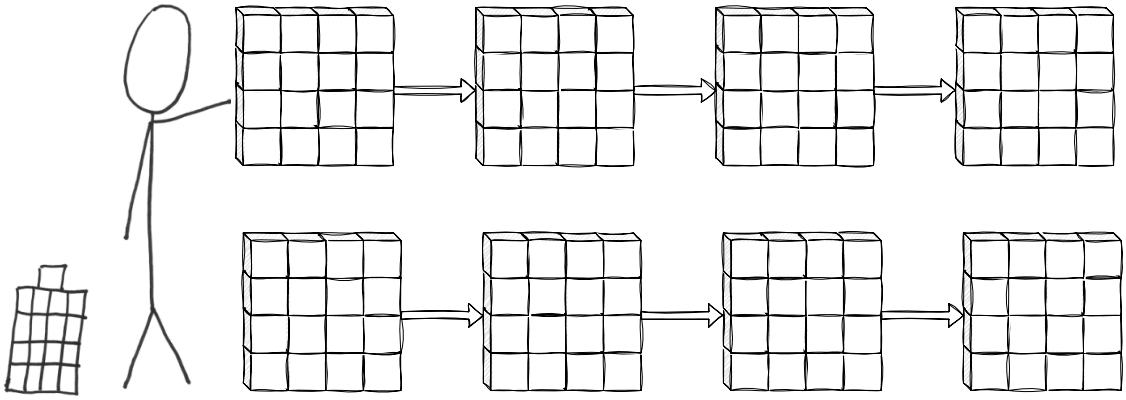
Student's Name | Roll No. | | | | | | | | |

- Instructions
  - Answer in the space provided and show steps whenever applicable.
  - Use rough sheet for supplementary work
  - Attach it with this answer script

1. Recall the following statement from the Stick-Figure Guide to AES.

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

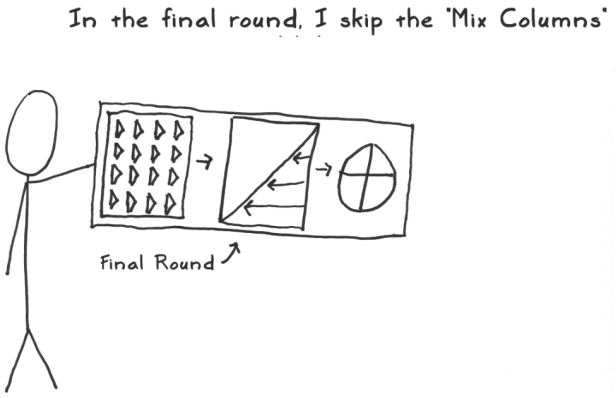
(a) Justify the statement pictorially using the state diagram below. [4]



(b) State the theorem related to AES that you used for Part (a). [3]

(c) What is meant by a truncated differential? Give an example. [3]

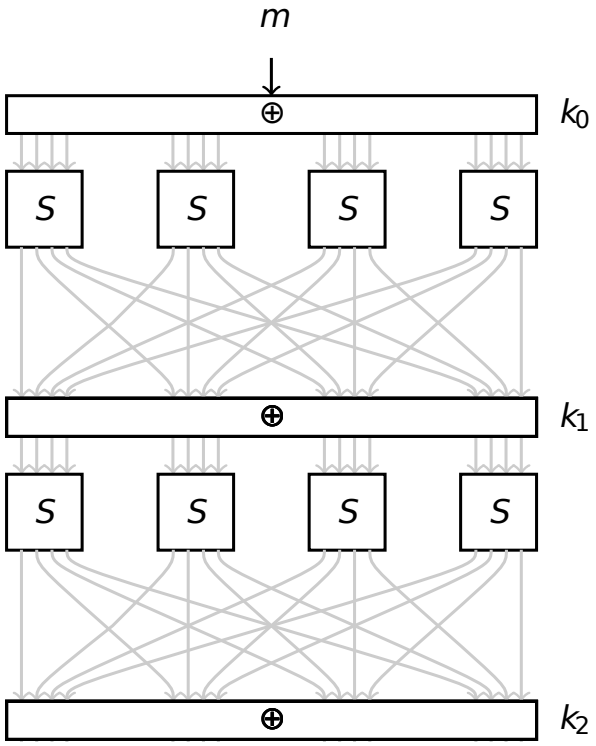
2. (a) Explain the implication of the following statement considering both the **software** and **hardware** implementations of AES. [7]



(b) How many rounds are there in various AES variants? [3]

3. (a) Consider the following DDT you saw in class. Find a characteristic such that total number of active SBox-es is **exactly** 5. Highlight it in the figure (use a pencil if needed). Show the step-by-step computation of its probability? [5+3]

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



Probability Calculation:

(b) Define differential uniformity (DU)? What is the DU of the SBox corresponding to the DDT given above? State the transition that leads to it. Why are the values even? [2+1+1+3]

4. (a) A cryptosystem has perfect secrecy if $\mathbf{Pr}[x|y] = \mathbf{Pr}[x]$ for all $x \in \mathcal{P}, y \in \mathcal{C}$. What do you interpret by this? [5]

(b) Suppose Alice encrypts two plaintexts m and m' using OTP with the same key k. What information about m and m' is leaked to Eve (assume Eve knows that Alice has reused k)? A precise answer is expected! [5]

(c) 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]

5. (a) 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. [5]

(b) The one-time pad encryption of plaintext *iitbh* (written in ASCII: 8-bit encoding, e.g., $a \rightarrow 97$) under key k is:

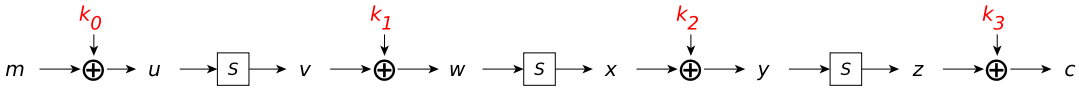
10000100 00000111 01010100 00011100 00011101

What is the one-time pad encryption of *crypt* under the same key? [10]

6. a) Which attack models do Differential and Linear Cryptanalysis belong to? [2]

b) In class it was said that Linear Cryptanalysis recovers 1-bit of key material. What is meant by that? [3]

c) List the steps if Linear Cryptanalysis is mounted from the plaintext side instead of ciphertext side in Sypher00C? [8]

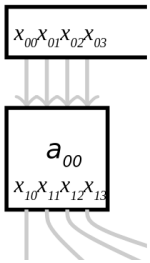


d) How many counters would be required for the above attack if we have a $b-$bit Sbox? [2]

7. a) What is a constrained optimization problem? What are its various components? [4]

b) Explain the following constraints. Which invalid paths does it avoid? [6]

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



8. Expand the following acronyms. $[1 \times 10]$

a) AES -

b) DDT -

c) LAT -

d) MDS -

e) CCA -

f) COA -

g) CBC -

h) ECB -

i) MILP -

j) SB $\rightarrow$ SR $\rightarrow$ MC -

---

6. (a) What are the security requirements of MACs and PRFs. [4+1+5]

(b) Do MACS have $\begin{pmatrix} \square \text{ stronger} \\ \square \text{ weaker} \end{pmatrix}$ security requirements than a PRF. Illustrate with a proof?

5]

7. (a) For the affine cipher, the multiplicative inverse of an element modulo 26 can be found as [3+2+3+2]

$$a^{-1} = a^{11} \bmod 26$$

Derive this using Euler's Theorem.

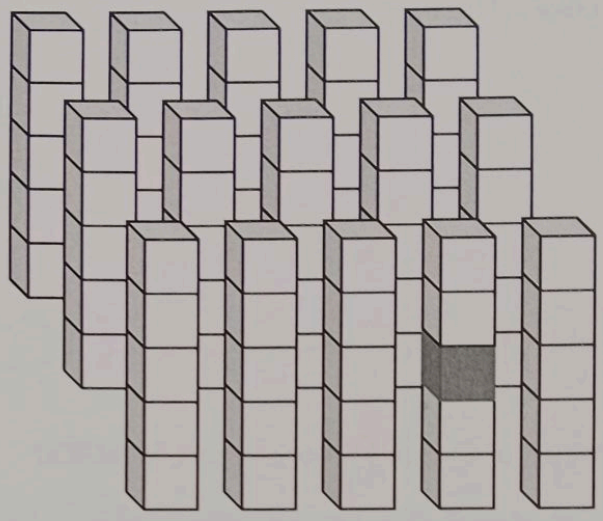
(b) Give a formal definition of Chosen Message Attack for MACs?

(c) Show that textbook RSA encryption is malleable. How do you fix the same?

(d) Are RSA signatures the converse of encryption?

8. Recall the θ operation in the SHA-3 Round function. The following figure shows a 3-slice version of the internal state. [3+2+3+2]

(a) Shade the columns on which the θ of the shaded cell relies on.



(b) Write the expression for theta in terms of three coordinates $(row,\ column,\ lane)$ considering the 3-dimensional matrix.

(c) What is a parity plane with respect to the θ operation? How would you compute it.

(d) Give the expression of the χ function assuming input as $(x_0, \cdots x_4)$ and output as $(y_0, \cdots y_4)$.

$y_0 =$

$y_1 =$

$y_2 =$

$y_3 =$

$y_4 =$

9. (a) State Euler's theorem (ET) and Fermat's Little Theorem (FLT) and prove that FLT is a special case of ET. [2+2+2+2+2]

(b) State the steps of RSA Encryption.

(c) Show how factoring n implies breaking RSA.

10. (a) Demonstrate the problem with textbook RSA signatures. [4 + 4 + 2

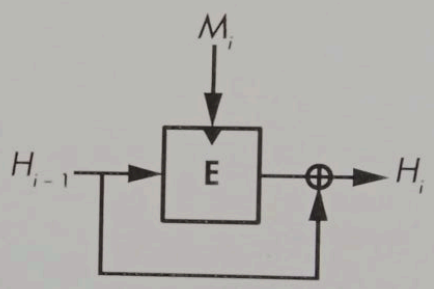
(b) Illustrate the technique to find multi-collisions using basic collisions.

(c) How many 2-collisions do you need to generate a $t-$multi-collision.

11. (a) Draw a block digram for the following hash functions built from a block cipher $e()$: [4+2+4]

- $e(x_i \oplus H_{i-1}, H_{i-1}) \oplus H_{i-1}$
- $e(H_{i-1}, x_i \oplus H_{i-1}) \oplus x_i \oplus H_{i-1}$

(b) The Davies-Meyer (DM) construction of designing hash functions from block ciphers is given below. First define what is a fixed point with respect to a hash function that uses chaining values. Now show how DM construction exhibits fixed-points



Department of Computer Science and Engineering
Indian Institute of Technology Bhilai

CS553/CSL505 – CRYPTOGRAPHY

End-Semester Exam
December 4, 2023

Time: 180 mins

Maximum Marks: $10 \times 12 = 120$

Student's Name

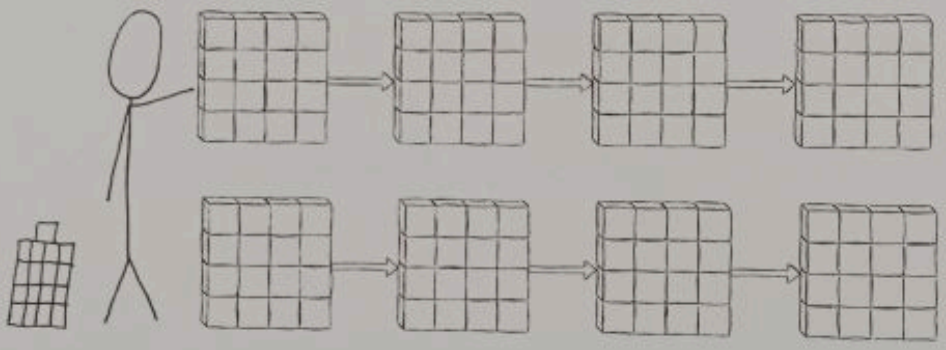
Roll No. | | | | | | | | |

- Instructions
  - Answer in the space provided and show steps whenever applicable.
  - Use rough sheet for supplementary work
  - Attach it with this answer script

1. Recall the following statement from the Stick-Figure Guide to AES.

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

(a) Justify the statement pictorially using the state diagram below. [4]



(b) State the theorem related to AES that you used for Part (a). [3]

(c) What is meant by a truncated differential? Give an example. [3]

12. Show the correctness of RSA: $d_{k_{pr}}(e_{k_{pub}}(x)) = x$. Use conventional notations: $(n, k_{pr}, k_{pub}, e, d, p, q)$. [10]

Student's name:

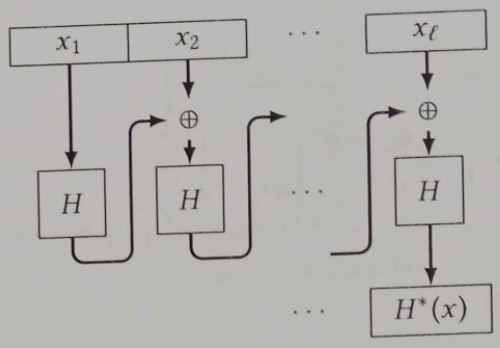
2. Derive the expression for the probability of finding a collision using using k out of n messages. [7 + 3]
   What is the value for Pr($Collison$) = $\frac{1}{4}$?

Student's name:

Please go on to the next page...

3] 3. (a) Let H be a collision-resistant hash function with output length n. Let H^* denote iterating H in a manner similar to CBC-MAC. [5+5]

$H^*(x_1 \cdots x_\ell)$:
// *each* x_i *is* n *bits*
$y_0 := 0^n$
for $i = 1$ to ℓ:
$y_i := H(x_i \oplus y_{i-1})$
return y_i



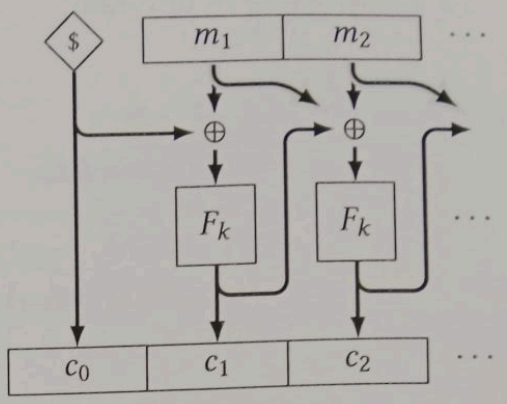
Describe an attack to show that H^* is **not** collision-resistant.

(b) Complete the table using Yes/No (Y/N)

Mode of Operation	Property: Stream Mode	Property: Parallelizable Encryption	Property: Random Access Decryption
CBC			
CFB			
OFB			
CTR			

4. Propagating CBC (PCBC) mode refers to the following variant of CBC mode ($blen \rightarrow$ block-length): [6+4]

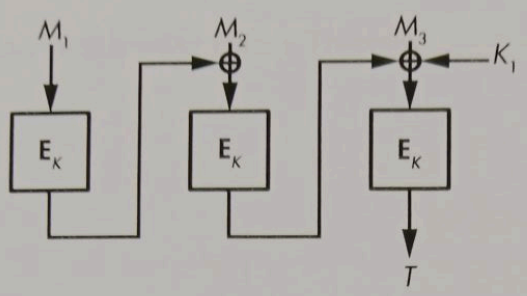
$\underline{\text{Enc}(k, m_1 \cdots m_\ell)}$:
$c_0 \leftarrow \{0,1\}^{blen}$;
$m_0 := 0^{blen}$
for $i = 1$ to ℓ:
  $c_i := F(k, m_i \oplus c_{i-1} \oplus m_{i-1})$
return $c_0 c_1 \cdots c_\ell$

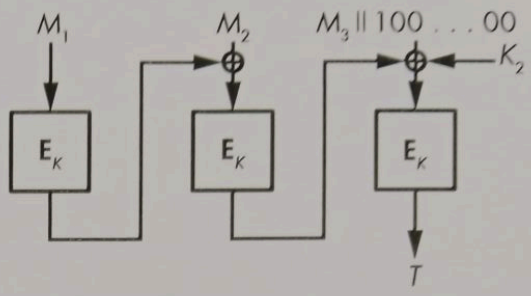


a) Draw the diagram and write the pseudo-code for PCBC Decryption.

b) Do an error propagation analysis for PCBC mode.

5. (a) Demonstrate a forgery attack to justify why C-MAC uses two different keys based on M being a sequence of integral blocks or not. [5+5]





(b) Expand the following:

- MAC
- PRF
- OEAP
- PSS
- RSA

Student's name: