Department of Computer Science and Engineering
Indian Institute of Technology Bhilai
CS553/CS(L)305 — **CRYPTOGRAPHY**

Mid Semester Exam
October 5, 2023

Time: 120 mins. Maximum Marks: [illegible]

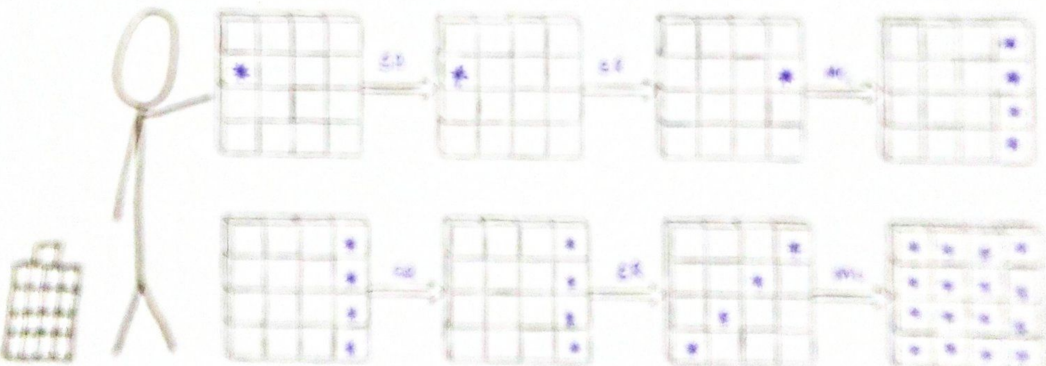
Student's Name: [illegible] Roll No. [illegible]

- Instructions
  - Answer in the space provided and show steps wherever applicable
  - Use rough sheet for supplementary work
  - Attach it with the 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]

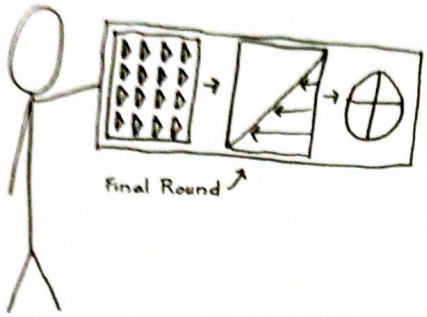
The theorem is that changing one bit in input can take effect and change multiple bits in the output. Also known as avalanche effect.

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

0

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

In the final round, I skip the 'Mix Columns'



→ ~~Soln~~ Ans In Mix Columns, we multiply the matrix with another matrix to get diffusion. But, for the final round, even if we create diffusion it would not create change in ~~finding~~ the probability. ~~of~~

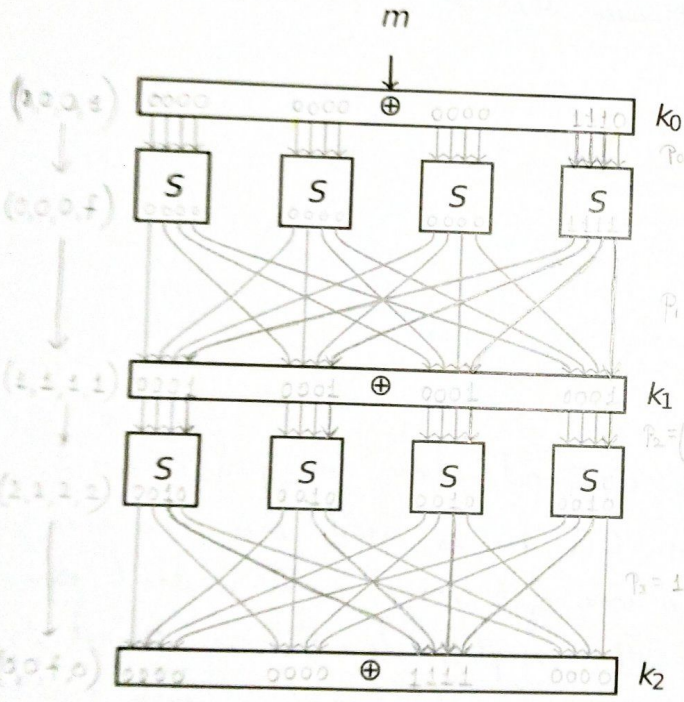
While in hardware implementation, 2 0

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

→ in ~~128 bit~~ AES-128, there are 9 rounds
In AES-192, there are 11 rounds
in AES-256, there are 13 rounds

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	.	6	6	.	.	.	2	.	2	.	.	.	2	.	4	.
3	.	.	.	6	.	2	.	.	2	2	.	.	.	.	.	.
4	.	.	2	.	2	4	.	2	.	.	.	.	4	.	2	.
5	.	2	2	.	4	.	.	.	2	2	2	.	.	.	2	.
6	.	.	2	.	4	.	4	2	.	.	2	.	.	.	.	.
7	.	.	.	.	.	.	2	2	.	2	2	2	.	.	.	.
8	.	.	.	.	4	4	.	2	2	2	2	.	.	.	.	.
9	.	.	.	.	2	.	2	4	.	.	4	.	2	.	2	.
a	.	2	.	.	2	2	2	.	4	2	.	.	.	.	.	2
b	.	.	.	2	2	.	.	.	4	4	.	2	2	.	.	.
c	.	4	.	2	.	2	2	2	.	.	4	.	.	2	.	.
d	.	.	.	.	2	.	.	2	.	.	.	.	.	.	6	.
e	.	2	.	4	2	.	.	.	.	.	.	6	2	.	.	4
f	.	.	.	.	2	.	2	.	.	.	2	.	.	.	.	6
													10	.		2



Probability Calculation:

Total probability,

$P = P_0 \cdot P_1 \cdot P_2 \cdot P_3$

$= \left(\frac{6}{16}\right) \cdot 1 \cdot \left(\frac{6}{16}\right)^4 \cdot 1$

$\therefore \boxed{P = \left(\frac{6}{16}\right)^5}$

8

(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]

Differential uniformity is the maximum no. of times a input difference is equal to output difference. The DU corresponding to DDT is 10. The transition is (f, d).

The values in DDT are even as sbox is bijective

4

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

→ the interpretation is that, even if the attacker knows the ciphertext y. he/she still can't deduce that x is the corresponding plaintext for ~~pb~~ ciphertext y.
The probability ~~that~~ after knowing ciphertext y & before knowing ciphertext is same.
Thus is no leak of information.

(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]

~~or~~ ~~Eve~~ ~~now~~ the only information that is leaked about m & m' is ~~that~~ their length.

(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]

→ There wouldn't be any significant change in perfect secrecy due to this decision as OTP key is used once, so even if ~~$e_k(m) = m$~~ plaintext is same after encryption, it wouldn't ~~even~~ help them in finding ~~other~~ other ~~one~~ plaintexts. Deciding ~~to~~ not to use $k = 0^n$, would just not let them know even a single plaintext in the ciphertext.

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]

For block-size n, total number of n-bit permutations are - $(2^n)! \approx \sqrt{2\pi n}\, n^n$ permutations

5

while the key has a key-size k,
∴ total number of possible permutations = 2^k

In the total of $(2^n)!$ permutations, only tiny fraction of available permutations ie 2^k can be possible key-values.

(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

4

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

→ ~~10000100 00000111 01010100 00011100 00011101~~

00111101	00111101	00101100	00100010	00101000
⊕ k_1	⊕ k_2	⊕ k_3	⊕ k_4	⊕ k_5
10000100	00000111	01010100	00011100	00011101

k_1 = 10111001
k_2 = 00111010
k_3 = 0111 1000
k_4 = 00111110
k_5 = 00110101

crypt → 00100011 00101010 00110001 00100001 00111101

\+ 10111001 00111010 01111000 00111110 00110101

10011010 00010000 01001001 00011111 00001000

Student's name:

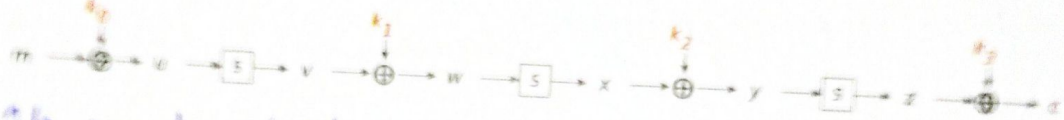
9. a) Which attack models do Differential and Linear Cryptanalysis belong to? [2]

→ They are block box attack models.

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

When a LC is used it finds out a linear relation between message & ciphertext bits and the key. Using it, we can get a bit of key material

c) List the steps if Linear Cryptanalysis is mounted from the plaintext side instead of ciphertext side in Sygher32C? [8]



We guess k_1, ~~$u \oplus k_0 = u$~~ ~~$v = xu' \oplus \ldots$~~

The equation we get here is -

$$\Rightarrow d.c \oplus d.v' = d.k_1 \oplus d.k_2 \oplus d.k_3$$

Here, we create two counters, T_0^i & T_1^i

if $d.c \oplus d.v' = 0$, then $T_0^i{}++$

if $d.c \oplus d.v' = 1$, then $T_1^i{}++$

d) How many counters would be required for the above attack if we have a 4-bit Sbox? [2]

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

→ The problem which can be optimized when it have equation when certain constraints are in cryptography

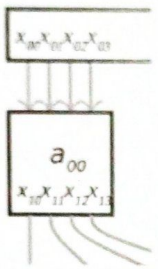
Components are -

1) set of variables
2) objective function
3) set of constraint

3

b) Explain the following constraints. Which invalid paths does it avoid? [5]

$$a_{x00} + a_{x01} + a_{x02} + a_{x03} - (x_{00} + x_{01} + x_{02} + x_{03}) \geq 0$$
$$a_{x00} + a_{x01} + a_{x02} + a_{x03} - (x_{10} + x_{11} + x_{12} + x_{13}) \geq 0$$



6

If one of x_{00}, x_{01}, x_{02} & x_{03} ~~are~~ is 1 & if ~~or~~ all x_0, x_1, x_2 & x_3 are 0, t this constraint fails.

It avoids this path. ~~this~~ ~~path~~ This constraint tells us that if any of x_{00}, x_{01}, x_{02} & x_{03} is 1 then there must be atleast ~~one~~ any one x_{10}, x_{11}, x_{12} & where value is 1 i.e. an active sbox give an output which a has atleast one bit which is 1.

It avoid such situation when an active sbox gives output 0 as it sho not be possible for an sbox to give output as 0.

8. Expand the following acronyms. [1 × 10]

(9)

a) AES - Advanced Encryption Standard

b) DDT - ~~Distribution~~ Differential Distribution Table

c) LAT - Linear Approximation Table

d) MDS - Mixed Differential Substitution

e) CCA - Chosen Ciphertext Attack

f) COA - Ciphertext Only Attack

g) CBC - Cipher Block Chaining

h) ECB - Electronic Code Book

i) MILP - Mixed-Integer Linear Programming

j) SB → SR → MC - Substitution Bytes → Shift Rows → Mixed Column

Department of Computer Science and Engineering
Indian Institute of Technology Bhilai
CS353/CSL505 – **CRYPTOGRAPHY**

End Semester Exam
December 4, 2023

Time: 180 mins | Maximum Marks: $10 \times 12 = 120$

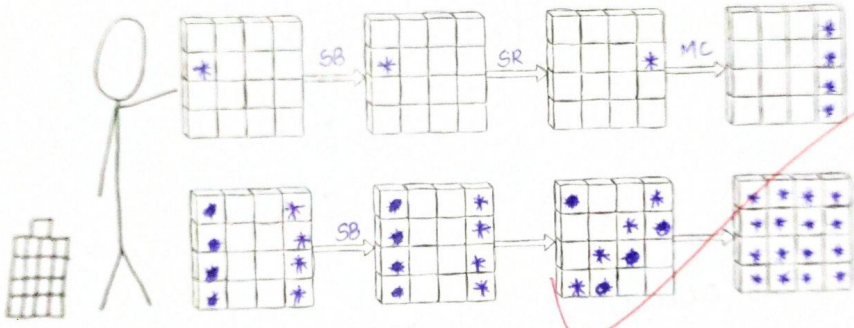
Student's Name: Sanket Dandge | Roll No: 1 2 1 4 0 5 4 0

- Instructions
  - Answer in the space provided and show steps wherever 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]

→ The theorem used is MDS theorem i.e Maximum Difference Separable. It states that if any state is active, then its effect can take place on more than one block for the next round.

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

→ Truncated differential means that we are not concerned with the output of the difference but with the difference itself.

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

→ $e^x = 1 - \frac{x}{1!} + \frac{x^2}{2!} - \frac{x^3}{3!} + \dots$

as $x \to 0$, $e^x \to 1-x$

$\Pr(\text{Collision}) = 1 - \Pr(\text{No collision})$

$= 1 - \left(\frac{n}{n} \cdot \frac{n-1}{n} \cdot \frac{n-2}{n} \dots \frac{n-(k-1)}{n}\right)$

$= 1 - \left(1 \cdot \left(1-\frac{1}{n}\right) \cdot \left(1-\frac{2}{n}\right) \dots \left(1-\frac{(k-1)}{n}\right)\right)$

$= 1 - \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right)$

$= 1 - \prod_{i=1}^{k-1} e^{-i/n} = 1 - e^{\sum_{i=1}^{k-1} -i/n}$

$1 - e^{-n\left(\frac{k(k-1)}{2}\right)}$

$= 1 - e^{-k^2/2n}$

10

if $\Pr(\text{collision}) = 1/4$

$\therefore \frac{1}{4} = 1 - e^{-k^2/2n}$

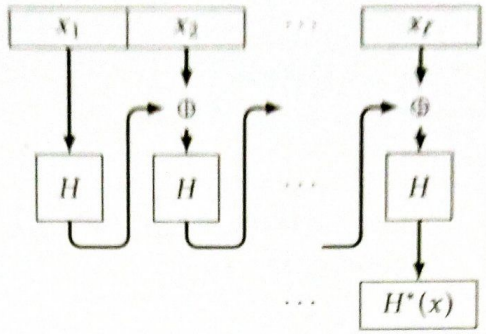
$e^{-k^2/2n} = 1 - \frac{1}{4} = \frac{3}{4}$

$-\frac{k^2}{2n} = \ln\left(\frac{3}{4}\right)$

$k = \sqrt{2n \ln\left(\frac{4}{3}\right)}$

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.

→ $H^*(x) = H(x_\ell \oplus H(y_{\ell-1}))$

If we change $x_\ell \to x_\ell \oplus y_{\ell-1}$

~~$H^*(x) = H(x_\ell \oplus y_{\ell-1} \oplus H(x_{\ell-1}))$~~

$H^*(x) = H(x_\ell \oplus$

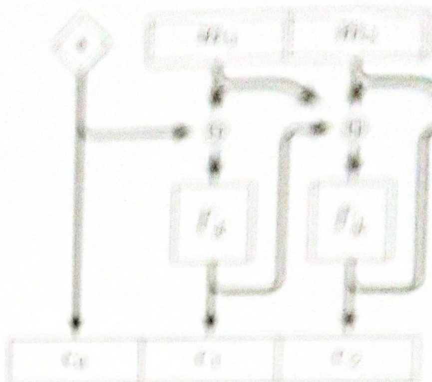
(b) Complete the table using Yes/No (Y/N)

4

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

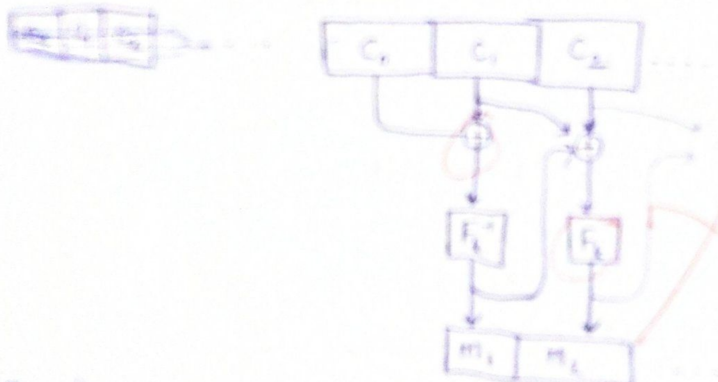
6. Propagating CBC (PCBC) mode refers to the following variant of CBC mode (blocklen = block length)

Enc$(k, m_1 \cdots m_\ell)$:
  $c_0 \leftarrow \{0,1\}^{blocklen}$
  $m_0 := 0^{blocklen}$
  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

→



Dec$(k, c_0, \ldots, c_\ell)$:
  $c_0 \leftarrow \{0,1\}^{blen}$
  $m_0 := 0^{blen}$
  for $i = 1$ to ℓ
    $m_i := F^{-1}(k, m_{i-1} \oplus c_{i-1} \oplus c_i)$
  return $m_1 m_2 \ldots m_\ell$

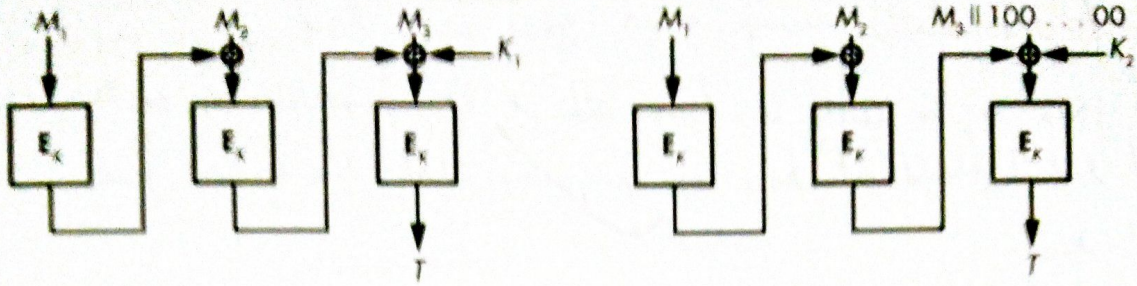
1

b) Do an error propagation analysis for PCBC mode

→ If bit is flipped in any c_i, then the entire m_i message will be garbled and all m_{i+1} will be garbled as well resulting in complete garbled message through the end

4

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 – Message Authentication Code
- PRF – Pseudo Random function
- OEAP – Optimal Assymmetric Encryption Padding
- PSS –
- RSA – Rivest - Shamir - Adleman

4

Student's name:

6 (a) What are the security requirements of MACs and PRFs

→ MACs require no reuse of key as it can be used for forging another message which gives same hash.

(2)

PRFs require itself to have all the properties of true random function but it should not have any properties that true random function doesn't have.

(b) Do MACS have (☐ stronger ☑ weaker) security requirements than a PRF. Illustrate with a proof?

→ PRF (Pseudorandom function) are functions which ensures that there is no properties that it has which a true random function does not have i.e they must look random.

If the hash is random, then there is no way to do forgery. And if no forgery possible then MAC is secure as well.

It tells that PRFs is stronger than MACs.

(6)

And if we take converse, if forgery is found in the MAC then the MAC fails but it doesn't mean that PRF fails as well.

PRF2 → Hash(PRF1) from PRF1 → Hash(PRF)

↳ PRF2 → Hash(PRF1||0)

which is true is not pseudorandom anymore. So, it doesn't fail.

∴ we can say MACs have weaker security requirements than PRF

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

→ $n = 26 \Rightarrow n = p \cdot q = 2 \cdot 13$

$\phi(n) = (p-1)(q-1) = 12 \cdot 1 = 12$

Taking $x = n$

~~$x = e \bmod (\phi(n))$~~ $y = a^{11} \bmod 26$

$\because d \cdot e = 1 \bmod (\phi(n)) \Rightarrow d$ is inverse of e

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

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

→ In this attack, message is chosen in such a way & added to previous message that it gives error which can be exploited to make another message having same hash (forgery).

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

→ $y_1 = x_1^e \bmod n$

$y_2 = x_2^e \bmod n$

$y = y_1 \cdot y_2 = (x_1 \cdot x_2)^e \bmod n$ ✓ (2)

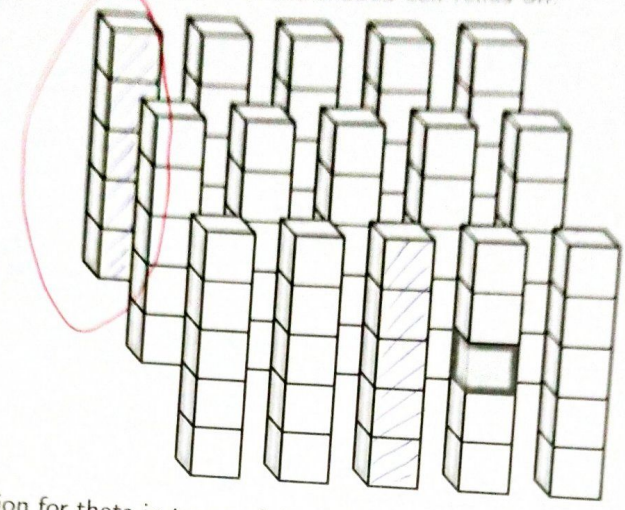
∴ Get new P-C pair, showing textbook RSA encryption is malleable

(d) Are RSA signatures the converse of encryption?

→ RSA signatures are the converse of encryption as the private key is used to sign the message & to get a unique hash

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+

(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 $(y_0, \cdots y_4)$.

$y_0 = x_0 \oplus (\sim x_4 \wedge x_0)$

$y_1 = x_1 \oplus (\sim x_0 \wedge x_1)$

$y_2 = x_2 \oplus (\sim x_1 \wedge x_2)$

$y_3 = x_3 \oplus (\sim x_2 \wedge x_3)$

$y_4 = x_4 \oplus (\sim x_3 \wedge x_4)$

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]

→ Euler's theorem states that GCD of any two numbers can be reduced to GCD of 2nd number & 1st number modulo 2nd number where 1st number > 2nd number.

$gcd(r_0, r_1) = gcd(r_1, r_0 \bmod r_1)$

Fermat's Little Theorem states that $a^{\phi(n)} = a$

2 0

(b) State the steps of RSA Encryption.

→ i) Choose any p & q which are two large primes

ii) $n = p \cdot q$

iii) Find $\phi(n) = (p-1)(q-1)$

iv) ~~$d \cdot e = \bmod(\phi(n))$~~ choose any value of e.

v) $d \cdot e = \bmod(\phi(n))$, find d.

vi) Use it in equ^n, $y = x^e \bmod n$ where $k_{pub} = (n, e)$ & x → plaintext & y → ciphertext

1

(c) Show how factoring n implies breaking RSA.

→ This problem refers to integer factorization problem which says that product of two large prime is easy but it is hard to finding the factors for $p \cdot q (= n)$.

Here, $n = p \cdot q$ but here p & q are unknown. Then we find $\phi(n)$

$\phi(n)$ can be calculated only by factorizing n into p & q & then finding $\phi(n) = (p-1)(q-1)$ which then helps in finding d & e as $d \cdot e = \bmod(\phi(n))$.

Therefore factoring n implies breaking RSA.

2

Student's name:

10 (a) Demonstrate the problem with textbook RSA signatures

→ Thus we have signatures -

$y_1 = x_1^e \bmod n$

$y_2 = x_2^e \bmod n$

$y_1 \cdot y_2 = (x_1 x_2)^e \bmod n$

Thus two can be multiplied to get another signature-plaintext pair and can be exploited for getting information

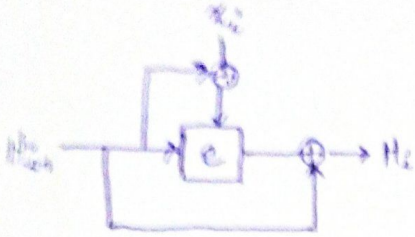
(b) Illustrate the technique to find multi-collisions using basic collisions.

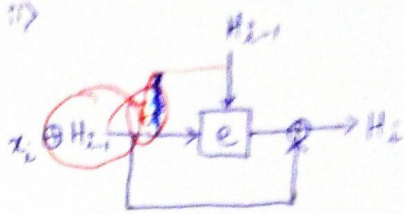
(c) How many 2-collisions do you need to generate a t-multi-collision

→ ${}^{t}C_2$ 2-collisions are needed to generate t-multi-collision.

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

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

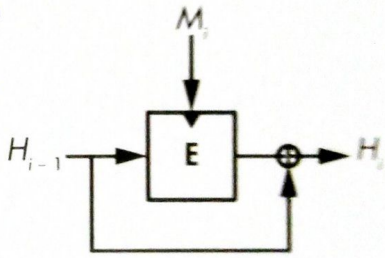




9

(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

→ The fixed point with respect to a hash function that uses chaining values is the point which gives same H_i ~~even~~ ~~when~~ for another message as well



The ⊕ expression will be -

$$H_i = H_{i-1} \oplus E(H_{i-1}, M_i)$$

To get fixed point, $H_i = H_{i-1}$

$$E(H_{i-1}, M_i) = 0$$

$$\therefore E(H_{i-1}, D(M_i, 0)) = 0$$

(message, key)

This is how, fixed point are exhibited in DM construction

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

→ Choose any ~~2~~ two large primes p & q.

Then, $n = p \cdot q \Rightarrow \phi(n) = (p-1)(q-1) \Rightarrow e \cdot d = \mod(\phi(n))$

For ~~finding~~ encryption function, use k_{pub} we get the equ^n

$$e_{k_{pub}}(x) = y = x^e \bmod n$$

For decryption function, use k_{pr}, we get the equ^n

$$d_{k_{pr}}(y) = x = y^d \bmod n$$

(7)

Now finding $d_{k_{pr}}(e_{k_{pub}}(x))$, we get

$$d_{k_{pr}}\left(e_{k_{pub}}(x)\right) = \left(x^e \bmod n\right)^d \bmod n$$

$$= x^{e \cdot d} \bmod n$$

$$= x^{1 \bmod (\phi(n))} \bmod n$$

We can say that $1 \bmod (\phi(n)) = 1$

$$\therefore = x \bmod n$$

$$= x$$

$$\therefore d_{k_{pr}}\left(e_{k_{pub}}(x)\right) = x$$

1 case missing