

Roll No: U19CS012

MID SEMESTER EXAM

Name: BHAGYA VINOD RANA

No. of Pages: 10

Date of Exam 11/03/2022

①

① Student Grade information - Moderate Impact

Only student's roll no & marks are shared, but no email & contact details, but it has serious adverse effect

② Electronic Health record of patient - HIGH

this is sensitive confidential info between doctor & patient & can be used to threaten / plan murder against the patient

③ Online forum website - LOW

people are mostly anonymous for giving their views & poll.

④ Data Related to National security - HIGH

data of ~~the~~ nuclear codes & missiles is very imp & can't be compromised. Catastrophic impact

⑤ Customer credit card & PIN - HIGH

they can be used to issue fake credit cards / duplicate cards & perform carding / money theft.



2. > One time pad →

a b c d e f g h i j k l m n o p q r s t u v w x y z  
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

a) Message = "paynow"

Key = 231450

paynow ⇒  
p a y n o w  
15 0 24 13 14 22

key ⇒ 2 3 1 4 5 0

(Add & do mod 26)  $(15+2) \times 26$   $(0+3) \times 26$   $(24+1) \times 26$   $(13+4) \times 26$   $(14+5) \times 26$   $(22+0) \times 26$   
17 3 25 17 19 22

Ans Ciphertext [ 17 3 25 17 19 22 ]

b) ciphertext 17 3 25 17 19 22

Plaintext

(key) 2 3 1 4 5 0

(do subtraction)  $(17-2) \times 26$   $(3-3) \times 26$   $(25-1) \times 26$   $(17-4) \times 26$   $(19-5) \times 26$   $(22-0) \times 26$

26 - 11 = 15  
15 15 6 4 5 0

Ans \* Key [ e p g e f a ]



3> n bit

$n = 128 \text{ bits} \rightarrow$

Attacker = 50 numbers  $\rightarrow$  1's  
 $128 - 50 = 78$  0's

BRUTE force

$$\frac{(128)!}{(50!)(78)!} \rightarrow [1.12 \times (e^{36})]$$

a) Substitution cipher [replace plain text  $\rightarrow$ ]

① we can do frequency analysis of block (cipher) letter

- ① 1-to 1 unique mapping
- ② frequency of letters in english language
- ③ ~~language~~  
 $(2^{50})$  combinations

(finite time)  
 (can be cracked)

$\rightarrow$  It does not change the number of 1's

b) Permutation cipher

try out all the permutation of all letters of alphabet & convert it into binary & then use it as dictionary to decrypt the cipher

It's same as substitution cipher, since permutations are not increasing 1's

c) combination of subs + permutation cipher

~~It's very hard to~~ Same  $\Rightarrow \frac{(128)!}{50!78!}$  (same time taken)  
 substitution  $\rightarrow$  permutation  $\rightarrow$  no extra calc needed)



4)

PA.

We observe: change in single bit of plain text, effects

Avalanche effect - means small change in plain text ~~text~~ should create significant change in ciphertext

DES is has been proved to be strong with regard to this property.

Plain  $\rightarrow$  0000 0000 0000 0000

Cipher  $\rightarrow$  4789 FD47 CE 82 ASF1

Plain  $\rightarrow$  0000 0000 0000 0001

Cipher  $\rightarrow$  0A4E D5C1 5A63 FEA3

Key used is same

key = 2213 4512 987A BB23

Although, the two plain text differ only in 1 bit,

ciphertext block differs a lot / significantly.

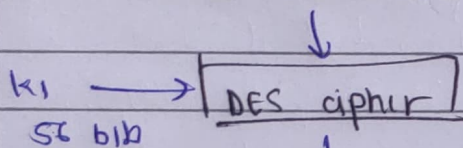


5) Double DES for Brute force & Meet in the Middle① Brute force  $\Rightarrow$  uses DES twice

$$\text{Key} = 2 \times (56 + 56) = 112 \text{ bit key}$$

$$\text{Security} = 2 \times 2^{56} = \boxed{2^{57}} \text{ combination of key's to be security } (2^{56} < 10^{17})$$

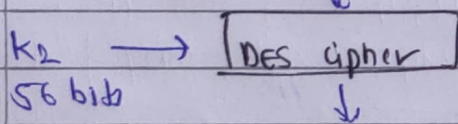
64 bit Plaintext



$$P \rightarrow E(K_1, P)$$

$$E(K_2, E(K_1, P)) = \text{Cipher}$$

(64 bit middle text) temporary ciphertext



ciphertext

② Meet in the middle - This attack involves encryption from 1 end & decryption from other end and then

"matching the results in middle" & hence the name.

$$\text{Decrypt}(K_2, C) = \text{Encrypt}(K_1, P)$$

$\therefore (K_1, K_2)$  is key pair used.

(i) encrypt "P" for all  $2^{56}$  possible values of  $K_1$  & store result in table & sort it

(ii) Now decrypt "C" using all  $2^{56}$  possible values of  $K_2$ . As a ~~result~~ decryption, check against table for match.

(iii) When there is match we pair the key, & try for all possible pair of keys.

\*

Triple DES - No more men in middle attack

→ Another

$$\text{Security} = (56 + 56 + 56) = 168 = \text{Key}$$

$$2^{56} \times 2 \times 2 = [2^{58} \text{ security}]$$

Key ↑ & Security ↑

DES cipher

DES cipher

$$\text{Decrypt}(C, K) = \text{Encrypt}(K, P)$$