CS362 CRYPTOGRAPHY U19CS012

Roll No: U19CS012 MID SEMESTER EXAM

Name: BHAGYA VINOD RANA No. of Pages:

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 ~~su~~ ~~but~~ 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.

vision

UI19CS012

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

	p	a	y	n	o	w
paynow ⇒	15	0	24	13	14	22
numbers						
key ⇒	2	3	1	4	5	0
(Add & do mod 26)	(17 % 26)	(3 % 26)	(25 % 26)	(17 % 26)	(19 % 26)	(22 % 26)
	17	3	25	17	19	22

Ans Ciphertext [r d z r t w]

b) ciphertext r d z r t w
(~~key~~) 17 3 25 17 19 22

Plaintext
(~~key~~) is n o t n o w
13 14 19 13 14 22

(+26) (do subtraction) (3-14)×26 (17-13)×26 0×26
(17-13)×26 (25-19)×26 (19-14)×26
4 15 6 4 5 0

26 -11 = 15 (15)

Ans * key [e p g e f a]

U19CS012

3> n bit (n=128 bit) → $[1.12 \times (e^{36})]$

$\frac{(128)!}{(50!)(78!)}$

Attacker = 50 numbers → 1's
128 - 50 = 78 0's
(BRUTE force)

a) Substitution cipher [replace plain text →

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

① 1-to-1 unique mapping
② frequency of letters in english language
③ ~~tongue~~

(2^{50}) combination (finite time)

It does not change the number of 1's (can be cracked)

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 very hard to~~ Same ⇒ $\frac{(128)!}{50!78!}$ } (same time taken)

substitution → permutation → (no extra calc needed)

U19CS012

4) ~~P.E.~~

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 ⊖ → 0000 0000 0000 0000
Cipher → 4789 FD47 CE82 A5F1

Plain → 0000 0000 0000 0001
Cipher → 0A4E D5C1 8A63 FEA3

Key used is same
Key = 2243 4512 987A BB23

Although, the two plain text differ only in 1 bit, cipher text block differs a lot / significantly.

U19CS012

5) Double DES for Brute force & Meet in the middle

① Brute force ⇒ uses DES twice

Key = (56+56) = 112 bit key

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

64 bit Plain text

K_1 (56 bit) → DES cipher

(64 bit middle text) temporary ciphertext or

K_2 (56 bit) → DES cipher

ciphertext

$P \rightarrow E(K_1, P)$

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

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.

U19CS012

★

Triple DES - No more meet-in-middle attack

⇒ ~~Another~~

Security = (56+56+56) = 168 key

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

key ↑ & security ↑)