CRYPTONITE WITE-UP:

AVANISH MONEY SRIVATS

CONTENTS:

→MODULAR ARITHMETIC(FROM L-2 OF CHIRSTOFF PARR)

→ QUESTIONS SOLVED FROM CRYPTOHACK

→ BASIC INTRODUCTION TO CONCEPTS DONE FOR CRYPTOHACK

→ KNOWLEDGE GAINED FROM TEXT SOURCES (PEARSON,McGRAW HILL)

# MODULAR ARITHMETIC AND HISTORICAL CIPHERS:

## MODULAR ARITHMETIC:

GOAL: computation in finite sets  
  
EX- for a finite set in day to day:  
can be represented in a circle  
no. of hours(b/w 1-24hrs)  
in the example of 20 hr affer 12,we get mod24(12+20)=8  
we get this byb 30/24 which gives 8 as remainder  
  
  
LET a,r,m belong to Z and m>0  
we write   
  
m is the modulus and r is the remainder   
  
a ≡ R mod m  
  
if m divides (a-r),   
i.e: m|(a-r)  
  
ex) a=13 m=9  
r=4  
or 13 = 4mod9  
  
a-r = 13-4 =9   
which is divisble by m (9)   
  
  
**1A)COMPUTATION OF THE REMAINDER:**  
GIVEN:  
a,m belong to Z  
  
a=m  
  
a = q(m) + r ; quotient of m + remainder  
  
ex: a=42 m=9  
42 = 4(9)+ 6  
  
but also,  
42 = 3(9) + 15  
or   
42= 5(9) + (-3)  
both hold true  
so the remainder is not unique  
  
**1B)EQUIVALENCE CLASSES**ex- a=1=2 m=5  
  
12 = 2mod5 and 7mod5  
and -3mod5  
  
bcz 5|(12-2)or(12-7)or(12-(-3))all hold  
defining the infinite set  
{-3,2,7....} forms an equiuvalence class  
all members of the class behave equivalent modulo 5 in this example  
  
  
look at all equivalence classes  
modulo 5  
{..........-10,-5,0,5,10,15.......... }   
create classes containing -4,-3,-2,-1 also and then we have all infinite nos.  
we get 5 classses A,B,C,D,E  
we can create similair classes,  
  
this one class does not contain all integers,despite infinite members  
  
we have reduced infinte numbers with 5 nos from sets  
  
say we have a computation:  
13\*16-8=200  
200 = 0mod5   
now in th classes 13 lies in D, and 16 lies in B  
  
so D\*B -D  
all members of class behave equivalent  
so we can use any no in its equivalent class  
  
in this ex:  
13 replaced by 3,16 by 1  
and we get 0 again.  
IMMPORTANT APPLCATION:  
EX-3^8mod7  
we can do brute calculation or  
  
3^8= 81\*81= find equivalence classes for 7  
= 4\*4 = 2mod7

## RINGS: ALGEBRAIC VIEW ON MODULAR ARITHMETIC

prop of rings:  
1>foolows closure ppt.,result always inn the ring  
2> there is a neutral element 0 ,a+0 = a mod m  
3> for every a,thhere is -ve element -a, a+(-a) = 0mod m  
4> there is the neutral element 1 wrt multiplication , a\*(a^-1) = 1 mod m  
EX- for m=9 and a=2  
a inverse - 2\* (2^-1) = 1 mod9, it is not 1/2 as it does not lie in the ring  
it would work for say  
2\*5 = 1 mod 9  
2^-1 = 5mod9   
to test wehther an inverse exists  
we find gcd(if 1 then inverse exists else not) of no and m  
  
ex - 6 \* x = 7 mod 9  
gcd(6,9) not = 1 (its 3)  
HENCE INVERSE ONLY WORKS SOMETIMES.  
set of elements and set of operations,  
1> the set z index m = {0,1,2,3....m-1}  
2> two operators “+”and " \*" such that   
for all a,b,c belonging to Z  
1> a+b = cmod m  
2> a\*b= dmod m

# 3> SHIIFT(OR CAESAR ) CIPHER:

idea: shift letters in alphabet  
EX-  
K=3  
a → d  
b → e  
w→ z  
x→a (wrap around)  
wrap don with the help of modulo operator  
  
so encryption : x = x+ k mod 26  
  
2 ATTACKS:  
1> FREQUENCY ANALYSIS  
2>BRUTE FORCE ATTACk

# 4) AFFINE CIPHER

K = (A,B)  
y = A\*X + B mod 26  
y-b = a\*x mod 26  
x = a^-1 (y-b ) mod 26  
  
keyspace:  
#K   
#B=26,LOOKINIG AT DECRYPTION EQN. VALUES OF A IS LIMITED(ONLY EXISTS IF GCD EXISTS)  
IE:GCD(A,26) = 1  
#A = 12  
#K = $A\*#B=312  
  
  
  
MISCELLANEOUS IDEAS COVERED:

Applets and activeX controls

Programs that download onto the client while running the web page.

Execute inside browser.

Perform proccessing and periodically call for data from the server side.

COOKIES:

HTTP protocol → stateless

when client asks for a page- web server locates it and sends it→ forgets interaction

for continuous usage of server cookies are used-maintain the state of information

Web server sends the web browser a cookie.

This is stored in the clients hard disk.

Copy sent back to the server → used for identification

DIFFIE-HILLMAN KEY EXCHANGE ALGORITHM:

Used by 2 parties to agree on a key → key agreement

not encrypt,decrypt

steps:

A,B agree on 2 public large prime nos → A chooses random no. x

→ A = gxmod n → this sent to B → B does the same , B= gy mod n

→ B sent to A → A computes K1= BX mod n ; same for K2.

K1 = **K**2

MORE ON CIPHERS:

1> caeser cipher

2>mono-alphabetic cipher

3> homophonic sub’n cipher(more than one letter can be used to encrypt)

4>polygram sub’n cipher(blocks)

5>Vigenere cipher





