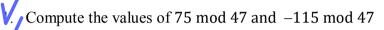
Introduction to Cryptography, Spring 2024

Homework 1

Due: 3/5/2024 (Tuesday)

Notes:

- (1) Show necessary steps of your computation in your homework. I don't want just the answers.
- (2) Submit a "hardcopy" right after the class on the due day. If you are not able to attend the class, submit it to EC238 before the due day. I don't accept late submission.



Use the extended Euclidean algorithm to solve the equation 235x + 53y = 1 for integers x and y

Use Euler's theorem to compute 23^{1562} mod 31 and 23^{1562} mod 35

Use the Rabin-Miller method to determine whether 133 and 137 are prime with confidence at least 98%?

Use CRT to solve the system of equations: $x \mod 4 = 2$, $x \mod 9 = 7$, $x \mod 11 = 5$, for integer x, $0 \le x \le 395$

Find all roots of $1 = x^{\phi(22)} \mod 22$ and compute their orders.

Use the baby-step-giant step algorithm to solve all possible values for $x = dlog_{5,23}(17)$

```
1_075=47+28(mod47)
     =28 (mod 47)
 @-115= 47x(-3)+ 26(mad 47)
      = 5P"
The solution of 23th+53y=1 TS
   (-23+53n,102-235n), where N∈Z, ¥
3. Euler's Thm.
    For a, n>0 and godla, w=1
    => a *(m) = ( (mod n), where $ (m) = # of numbers < N and
                                with qcd(n,\cdot)=1.
  () (300 (23,31)=1:23 = ((mad 31)) by Euler's Thm. (562 (562 mod 30)) =>23 = 23 (mod 31)
           (18 ban) PSZ = (18 ban) Esz
  = 2 (mod 31) & 24

= 2 (mod 31) & 24

= 23 = 1 (mod 3t) by Euler's Thm.
    =>53 = 53 (mad 35) = 23 (mad 35)
          =4 (max 35)
```

4. 1-14) > 98% =>4/k <0,02 => k> by 0.02 => 0.015625

(1) N=133 (1) N-1=132=2×33

(ii) Pick random Q=115 and compute

Q=33 mod N=115 mod 133 = 20 mod 133

Q=10d N=115 mod 133 = 1 mod 133

Q=10d N=115 mod 133 = 1 mod 133

=> 20 = 133-1 (mod 133), 20 = 1 (mod 133)

=> X=1 (mod 133) have non-trivial solutor

=) X2=((m=d133) have non-trivial solution =) 133 Brit a prime.

```
(2) N=137
  (2) N-1=136= 23x (1)
  (ii) Pick random Q=2 and compute
    Q' mad N = 2 mad 137 = 100 mad 137
    a nod N = 234 nod 137 = 136 nod 137
    017×22 mad N=268 mad 137 = 1 mad 137
    017 = 3 mad N= 236 mad 137 = 1 mad 137
    136 = 137- ( mad 137), (= ( (mad 137)
   >no solution are tound by a=2
  tiil Pick random Q=3 and compute
    Q' mad N = 3 mad 137 = 127 mad 137
    0 mod N = 334 mod 137 = 100 mod 137
    017×22 mad N=368 mad 137 =136 mad 137
    017 mad N=3136 mad 137 = 1 mad 137
    136= 137-1(mad 137)
   >no solution are tound by a=3
  biil Pick random Q= 7 and compute
    a' mad N = 7' mad 137 = 100 mad 137
    0 nod N=734 nod 137 = 136 nod 137

0 nod N=768 nod 137 = 1 nod 137

0 nod N=768 nod 137 = 1 nod 137

0 nod N=7136 nod 137 = 1 nod 137
    136 = 1377- ( ( wood 137), (= ( ( mod 137)
    >no solution are found by a=1
=>By Rubin-Miller alga, 137 is a prime with probability ≥98%
```

Step Trul
The solution for this equation is $X = 2 \times 99 \times 3 + 9 \times 44 \times 8 + 5 \times 36 \times 4 \pmod{396}$ $= 214_{44}$

(2)
$$ord_{22}(1) = ($$
 $ord_{22}(13) = (0$
 $ord_{22}(3) = 5$ $ord_{22}(15) = 5$
 $ord_{22}(5) = 5$ $ord_{22}(17) = 10$
 $ord_{22}(7) = (0$ $ord_{22}(19) = (0$

7. (t) m= [Jp]= [Jz]=5

(Ti)g= g(p-1)-m= 522-5= 57 (mod 23)

= 15 (mod 23)

(Tit) Find (T, J) Such that $C_1 = y(g^m)^2 \mod p$ $b_1 = g^2 \mod p$ $b_2 = g^2 \mod p$ Take (i,j) = (1,2)(iv) $X = i \times m + j = 1 \times 5 + 2 = 7$ Clog(17) = 7 Clog(17) = 7 Clog(17) = 7