列印成品

2024年3月5日　　上午 10:33

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.**

1. Compute the values of $75 \bmod 47$ and $-115 \bmod 47$
2. Use the extended Euclidean algorithm to solve the equation $235x + 53y = 1$ for integers x and y
3. Use Euler's theorem to compute $23^{1562} \bmod 31$ and $23^{1562} \bmod 35$
4. Use the Rabin-Miller method to determine whether 133 and 137 are prime with confidence at least 98%?
5. Use CRT to solve the system of equations: $x \bmod 4 = 2, x \bmod 9 = 7, x \bmod 11 = 5$, for integer x , $0 \leq x \leq 395$
6. Find all roots of $1 = x^{\Phi(22)} \bmod 22$ and compute their orders.
7. Use the baby-step-giant step algorithm to solve all possible values for $x = \mathrm{dlog}_{5,23}(17)$

Solutions

1. 28, 26

2.

i	r_i	q_i	x_i	y_i
-1	235		1	0
0	53		0	1
1	23	4	1	-4
2	7	2	-2	9
3	2	3	7	-31
4	1	3	-23	102

93

$\Rightarrow x = -23,\ y = 102$

3.
$$23^{1562} \bmod 31 = 23^{1562 \bmod \phi(31)} \bmod 31$$
$$= 23^{1562 \bmod 30} \bmod 31$$
$$= 23^2 \bmod 31$$
$$= 2$$

$$23^{1562} \bmod 35 = 23^{1562 \bmod \phi(35)} \bmod 35$$
$$= 23^{1562 \bmod 24} \bmod 35$$
$$= 23^2 \bmod 35$$
$$= 4$$

4. To have 98% confidence, we need

$\Pr[RM(n) = \text{non-prime} \mid n = \text{non-prime}] \geq 0.98$

Thus, we need $1 - (\frac{1}{4})^t \geq 0.98 \Rightarrow t \geq 3$

(a) $n = 133$

$n - 1 = 132 = 2^2 \cdot 33$

Random pick: $a = 2$

Random pick: $a=2$

Since $2^{133-1} \bmod 133 = 64 \neq 1$, n is not prime

(6) $n=137$,

$n-1 = 136 = 2^3 \cdot 17$

Random pick 3 a's: a_1, a_2, a_3

$a_1 = 12 \Rightarrow a_1^{17} \bmod 137 = 10$

$a_1^{34} \bmod 137 = 100$

$a_1^{68} \bmod 137 = 136 = -1$

$a_1^{136} \bmod 137 = 1$

$\Rightarrow a_1$ is not a witness for n being non-prime.

$a_2 = 30 \Rightarrow a_2^{17} \bmod 137 = 37$, $a_2^{34} \bmod 137 = 136 = -1$

$\Rightarrow a_2$ is not a witness

$a_3 = 7 \Rightarrow a_3^{17} \bmod 137 = 100$, $a_3^{34} \bmod 137 = 136 = -1$

$\Rightarrow a_3$ is not a witness

$\Rightarrow$ 137 is probability prime with confidence 98%

5. Use the CRT solution formula:

$x = 2 \cdot C_1 M_1 + 7 C_2 M_2 + 5 C_3 M_3 \bmod M$

$= 2 \cdot 3 \cdot 99 + 7 \cdot 8 \cdot 44 + 5 \cdot 4 \cdot 36 \bmod 396$

$= 214$

6. The roots of $1 = x^{\phi(22)} \bmod 22$

are $Z_{22}^* = \{1, 3, 5, \underline{7}, 9, \underline{13}, 15, \underline{17}, \underline{19}, 21\}$

Their orders are 1, 5, 5, 10, 5, 10, 5, 10, 10, 2.

[There are $\phi(\phi(22))$ primitive roots]

7. $5^x \equiv 17 \bmod 23$

7. $5^x \equiv 17 \mod 23$

By the baby-step-giant-step algorithm.

(a) $m = \lceil \sqrt{23} \rceil = 5$

(b) Compute $b_j = 5^j \mod 23$, $0 \le j \le 4$

$\Rightarrow b_0 = 1$, $b_1 = 5$, $b_2 = 2$, $b_3 = 10$, $b_4 = 4$

$a_i = 17 \cdot 5^{-5i}$, $0 \le i \le 4$

$\Rightarrow a_0 = 17$, $a_1 = 2$, $a_2 = 7$, $a_3 = 13$, $a_4 = 11$

Since $a_1 = b_2$, $x = 1 \cdot 5 + 2 \mod 22 = 7$