# 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 $x = \mathrm{dlog}_{5,23}(17)$

1. ① $75 \equiv 47+28 \pmod{47}$

$\equiv 28 \pmod{47}$ #

② $-115 \equiv 47\times(-3)+26 \pmod{47}$

$\equiv 26$ #

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 |
| 5 | 0 | 2 | | |

$\left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$ (商)

$y_{i-2}-(y_{i-1}\times q_i)$

$x_{i-2}-(x_{i-1}\times q_i)$

$r_{i-2}\%r_{i-1}$ (餘)

The solution of $235x+53y=1$ is

$(-23+53n, 102-235n)$, where $n\in\mathbb{Z}$. #

3. Euler's Thm.

For $a, n>0$ and $\gcd(a,n)=1$

$\Rightarrow a^{\phi(n)}\equiv 1 \pmod{n}$, where $\phi(n)$ = # of numbers $<n$ and with $\gcd(n,\cdot)=1$.

① $\because \gcd(23,31)=1, \therefore 23^{31-1}\equiv 23^{30}\equiv 1 \pmod{31}$ by Euler's Thm.

$\Rightarrow 23^{1562}\equiv 23^{1562 \bmod 30} \pmod{31}$

$\equiv 23^2 \pmod{31} \equiv 529 \pmod{31}$

$\equiv 2 \pmod{31}$ #

② $\because \gcd(23,35)=1, \therefore 23^{\phi(35)}\equiv 23^{24}\equiv 1 \pmod{35}$ by Euler's Thm.

$\Rightarrow 23^{1562}\equiv 23^{1562 \bmod 24} \pmod{35} \equiv 23^2 \pmod{35}$

$\equiv 4 \pmod{35}$

4. $1-(\frac{1}{4}) \geq 98\%$

$\Leftrightarrow (\frac{1}{4})^k \leq 0.02 \Leftrightarrow k \geq \log_{\frac{1}{4}} 0.02$

$\Rightarrow \underset{k}{\text{argmin}}\ k \geq \log_{\frac{1}{4}} 0.02 = 3.1, (\frac{1}{4})^3 = 0.015625$

(i) $n = 133$

(ii) $n-1 = 132 = 2^{r} \times 33^{d}$

(iii) Pick random $a = 115$ and compute

$a^{33} \bmod n \equiv 115^{33} \bmod 133 \equiv 20 \bmod 133$

$a^{33\times 2^1} \bmod n \equiv 115^{66} \bmod 133 \equiv 1 \bmod 133$

$a^{33\times 2^2} \bmod n \equiv 115^{132} \bmod 133 \equiv 1 \bmod 133$

$\Rightarrow 20 \not\equiv 133-1 \pmod{133}$, $20 \not\equiv 1 \pmod{133}$

$\Rightarrow x^2 \equiv 1 \pmod{133}$ have non-trivial solution

$\Rightarrow 133$ Isn't a prime.

(2) $n = 137$

(i) $n-1 = 136 = 2^3 \times 17$ ($r = 3$, $d = 17$)

(ii) Pick random $a = 2$ and compute

$a^{17} \bmod n \equiv 2^{17} \bmod 137 \equiv 100 \bmod 137$

$a^{17\times 2^1} \bmod n \equiv 2^{34} \bmod 137 \equiv 136 \bmod 137$

$a^{17\times 2^2} \bmod n \equiv 2^{68} \bmod 137 \equiv 1 \bmod 137$

$a^{17\times 2^3} \bmod n \equiv 2^{136} \bmod 137 = 1 \bmod 137$

$136 \equiv 137-1 \pmod{137}$, $1 \equiv 1 \pmod{137}$

$\Rightarrow$ no solution are found by $a = 2$

(iii) Pick random $a = 3$ and compute

$a^{17} \bmod n \equiv 3^{17} \bmod 137 \equiv 27 \bmod 137$

$a^{17\times 2^1} \bmod n \equiv 3^{34} \bmod 137 \equiv 100 \bmod 137$

$a^{17\times 2^2} \bmod n \equiv 3^{68} \bmod 137 \equiv 136 \bmod 137$

$a^{17\times 2^3} \bmod n \equiv 3^{136} \bmod 137 = 1 \bmod 137$

$136 \equiv 137-1 \pmod{137}$

$\Rightarrow$ no solution are found by $a = 3$

(iii) Pick random $a = 7$ and compute

$a^{17} \bmod n \equiv 7^{17} \bmod 137 \equiv 100 \bmod 137$

$a^{17\times 2^1} \bmod n \equiv 7^{34} \bmod 137 \equiv 136 \bmod 137$

$a^{17\times 2^2} \bmod n \equiv 7^{68} \bmod 137 \equiv 1 \bmod 137$

$a^{17\times 2^3} \bmod n \equiv 7^{136} \bmod 137 = 1 \bmod 137$

$136 \equiv 137-1 \pmod{137}$, $1 \equiv 1 \pmod{137}$

$\Rightarrow$ no solution are found by $a = 7$

$\Rightarrow$ By Rabin-Miller alga, 137 is a prime with probability $\geq 98\%$

5. Step1. Find $M$

$M = 4 \times 9 \times 11 = 396$

Step2 Find $M_i$

$M_1 = \frac{396}{4} = 99, M_2 = \frac{396}{9} = 44, M_3 = \frac{396}{11} = 36$

Step3. Find $c_i$ s.t. $c_i M_i \equiv 1 \pmod{m_i}$

$$\left.\begin{aligned} 3 \times 99 &\equiv 1 \pmod 4 \\ 8 \times 44 &\equiv 1 \pmod 9 \\ 4 \times 36 &\equiv 1 \pmod{11} \end{aligned}\right\} \Rightarrow \text{Take} \begin{cases} c_1 = 3 \\ c_2 = 8 \\ c_3 = 4 \end{cases}$$

Step Final

The solution for this equation is

$x = 2 \times 99 \times 3 + 7 \times 44 \times 8 + 5 \times 36 \times 4 \pmod{396}$

$= 214$ #

6. (1) $\phi(n)$ roots

= the set of $\mathbb{Z}_n^*$

$= \{x \mid 1 \le x \le n, \gcd(x, n) = 1\}$

$= \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$ □

(2) $\text{ord}_{22}(1) = 1$ $\quad \text{ord}_{22}(13) = 10$

$\text{ord}_{22}(3) = 5$ $\quad \text{ord}_{22}(15) = 5$

$\text{ord}_{22}(5) = 5$ $\quad \text{ord}_{22}(17) = 10$

$\text{ord}_{22}(7) = 10$ $\quad \text{ord}_{22}(19) = 10$

$\text{ord}_{22}(9) = 5$ $\quad \text{ord}_{22}(21) = 2$

□

7. (i) $m = \lceil \sqrt{p} \rceil = \lceil \sqrt{23} \rceil = 5$

(ii) $g^{-m} = g^{(p-1)-m} \equiv 5^{22-5} \equiv 5^{17} \pmod{23}$

$\equiv 15 \pmod{23}$

(iii) Find $(i, j)$ such that

$a_i = y(g^{-m})^i \bmod p$

$b_j = g^j \bmod p$

$\Rightarrow 17 \times 15^i \equiv 5^j \bmod 23$

Take $(i, j) = (1, 2)$

(iv) $X = i \times m + j = 1 \times 5 + 2 = 7$

$\text{dlog}_{5,23}(17) = 7$ //