CS326 – Systems Security

Mathematical Background 2

Elias Athanasopoulos
athanasopoulos.elias@ucy.ac.cy

Extended Euclidean Algorithm

- Find the modular multiplicative inverse of a

$$a \cdot x \equiv 1 \bmod m,$$

m and a are known, what is the value of x?

- Condition for existence: gcd(a, m) = 1 (i.e., a and m are co-primes)
- Example

$3x \equiv 1 \pmod{10}$

$3 \cdot 7 = 21 \equiv 1 \pmod{10}$

Algorithm

$a \cdot x \equiv 1 \bmod m$, then it holds that

$a \cdot x = 1 + k \cdot m$, for an integer k

or

$a \cdot x + (-k) \cdot m = 1$

If I can express x, m in the above form then I can compute "x"

Bezout's Identity: Let a and b be integers with gcd(a, b), there exist integers x and y such that $ax + by = \gcd(a, b)$

But, $\gcd(a, m) = 1 \Rightarrow a \cdot x + y \cdot m = 1$

(Diophantine Equation)

Example (1/3)

$$12 \cdot x \equiv 1 \pmod{67}$$

$$a = 12,\ m = 67$$

First, calculate the gcd()

gcd(67, 12) = gcd(67 – **5** · 12, 12) = gcd(7, 12) =
gcd(12, 7) = gcd(12 – **1** · 7, 7) = gcd(5, 7) =

gcd(7, 5) = gcd(7 – **1** · 5, 5) = gcd(2, 5) =

gcd(5, 2) = gcd(5 – **2** · 2, 2) = gcd(1, 2)
gcd(2, 1) = 1

Therefore, gcd(67, 12) = 1

Example (2/3)

- From the above calculations, it holds

$67 = 5 \cdot 12 + 7 \qquad (1)$

$12 = 1 \cdot \mathbf{7} + 5 \qquad (2)$

$7 = 1 \cdot \mathbf{5} + 2 \qquad (3)$

$5 = 2 \cdot \mathbf{2} + 1 \qquad (4)$

- Numbers in red are going to be substituted according to the above expressions

Example (3/3)

- It turns out, that

$1 = 5 - 2 \cdot \mathbf{2}$ *we substitute 2 from (3)*

$1 = \mathbf{5} - 2 \cdot (7 - \mathbf{5})$ *we substitute 5 from (2)*

$1 = 12 - \mathbf{7} - 2 \cdot (\mathbf{7} - 12 + \mathbf{7})$ *we substitute 7 from (1)*

$1 = 12 - (67 - 5 \cdot 12) - 2 \cdot (67 - 5 \cdot 12 - 12 + 67 - 5 \cdot 12)$

- Now, I have only 67 and 12 and I have to group their coefficients

$1 = 12 - 67 + 5 \cdot 12 - 2 \cdot (2 \cdot 67 - 11 \cdot 12)$

$1 = - 67 + 6\ 12 - 4 \cdot 67 + 22 \cdot 12$

$1 = - 5 \cdot 67 + 28 \cdot 12$

Solution

$$1 = -5 \cdot 67 + 28 \cdot 12$$

$$(\text{Recall: } 1 = (-5) \cdot m + 28 \cdot \alpha)$$

or

$$28 \cdot 12 = 1 + (-5) \cdot 67, \text{ i.e.,}$$

$$28 \cdot 12 \equiv 1 \pmod{67}$$

- The modular multiplicative inverse of $\alpha = 12$ and $m = 67$ is "28", or,

$$12^{-1} \equiv 28 \pmod{67}$$