CS326 – Systems Security

Mathematical Background 1

Elias Athanasopoulos
athanasopoulos.elias@ucy.ac.cy

Greatest Common Divisor gcd()

- $gcd(r_0, r_1) = ?$
- A solution is to factor r_0, r_1
- Then, the gcd should be the highest common factor
- Example
  - $r_0 = 84 = 2x\mathbf{2x3}x7$
  - $r_1 = 30 = \mathbf{2x3}x5$
  - $gcd(r_0, r_1) = 6$
- Factoring is complicated and hard for large numbers

Euclidean Algorithm

- It turns out that

  $\gcd(r_0, r_1) = \gcd(r_0 - r_1, r_1)$, where $r_0 > r_1$ and both r_0, r_1 are positives

- If we apply this recursively, several times

  $\gcd(r_0 - r_1, r_1) = \gcd(r_0 - r_1 - r_1, r_1) = \gcd(r_0 - 2r_1, r_1)$

  $\gcd(r_0 - 2r_1, r_1) = \gcd(r_0 - 2r_1 - r_1, r_1) = \gcd(r_0 - 3r_1, r_1)$

  ...

  $\gcd(r_0 - r_1, r_1) = ... = \gcd(r_0 - kr_1, r_1)$, where k is a positive integer, and $r_0 - kr_1 > 0$

Example

gcd(27, 21) = gcd(27 – 1x21, 21) =

gcd(6, 21) = gcd(21, 6) = gcd(21 – 3x6, 6) =
gcd(3, 6) = gcd(6, 3) = gcd(6-2x3, 3) =
gcd(0, 3) = gcd(3, 0)

Therefore, gcd(27, 21) = 3

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

$3x \equiv 1 \bmod 10$

$3 \cdot 7 = 21 \equiv 1 \bmod 10$

Euler's Phi Function, *Φ()*

- Assume a set of m integers, {0, 1, 2, ..., m-1}
- How many numbers in the set are relative primes to (or, *co-primes with*) m?
- Example, m = 6, {0, 1, 2, 3, 4, 5}

  gcd(6, 0) = 6

  gcd(6, 1) = 1

  gcd(6, 2) = 2

  gcd(6, 3) = 3

  gcd(6, 4) = 2

  gcd(6, 5) = 1
- Count the red lines, *Φ(6)* = 2

Calculating *Φ()*

- For large *m*, *Φ(m)* is hard to be calculated unless *m* can be expressed as a product of prime factors

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}$$

- Then,

$$\Phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1})$$

Example

- $m = 240 = 16 \cdot 15 = 2^4 \cdot 3 \cdot 5$

$\Phi(m) = (2^4 - 2^3)(3^1 - 3^0)(5^1 - 5^0) = 8 \cdot 2 \cdot 4 = 64$

- In the case that $m = p \cdot q$, i.e., $m = p^1 \cdot q^1$,

then $\Phi(m) = (p^1 - p^0)(q^1 - q^0) = (p - 1)\,(q - 1)$

- If m is a prime, i.e., $m = p^1$,

then $\Phi(m) = \Phi(p) = (p^1 - p^0) = (p - 1)$

Euler's Theorem

$$\alpha^{\varphi(m)} \equiv 1 \pmod{m}$$

only when $\gcd(\alpha, m) = 1$

- Example, $m = 12$, $\alpha = 5$

  $\Phi(12) = \Phi(2^2\, 3) = (2^2 - 2^1)(3^1 - 3^0) =$
  $= (4 - 2)\,(3 - 1) = 4$

  thus, $5^4 = 25^2 = 625 = 52 \cdot 12 + 1 \equiv 1 \pmod{12}$