Kryptografia i bezpieczeństwo systemów informatycznych

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. letni 2025/2026

inf.ug.edu.pl/~amb/

Kryptografia klucza publicznego Implementacja idei

Teoria grup

- zbiór G z działaniem
  – zapis np. $a + b$, albo $a \cdot b$, albo $a \bullet b$
  – istnieje „jedynka" e: $a \bullet e = e \bullet a = a$
  – łączność: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$
  – istnieją elementy odwrotne: $\forall a.\, \exists b.\, a \bullet b = e$, zapis a^{-1}
  – dla nas ważne będą wyłącznie grupy przemienne: $a \bullet b = b \bullet a$
- grupa skończona: rząd grupy = liczebność grupy $|G|$
- przykłady:
  – liczby całkowite i dodawanie, rząd nieskończony
  – reszty mod N i dodawanie: grupa addytywna $\mathbb{Z}_N = \{0, .., N-1\}$, $a \bullet b = a + b \mod N$, rząd $|\mathbb{Z}_N| = N$
  – niezerowe reszty mod p i mnożenie: grupa multiplikatywna $\mathbb{Z}_p^* = \{1, .., p-1\}$, $a \bullet b = a \cdot b \mod p$, rząd $|Z_p^*| = p - 1$
  – również grupa multiplikatywna $\mathbb{Z}_N^*$ – elementy odwracalne mod N, rząd grupy – funkcja Eulera $\varphi(N)$

Teoria grup, c.d.

- Potęgowanie
  – $a \in G$, n – liczba, $a^n = a \bullet a \ldots \bullet a$ (n krotnie)
- Tw.: $a^{|G|} = e$
  – dw.: mnożymy wszystkie elementy grupy $a_1 \bullet a_2 \bullet \ldots \bullet a_n$, $n = |G|$, a potem jeszcze raz pomnożone przez a:
  $(a \bullet a_1) \bullet (a \bullet a_2) \bullet \ldots \bullet (a \bullet a_n)$
  – To są te same elementy, tylko kolejność inna,
  – po skróceniu $a^n = e$
- Wn.: potęgowanie w grupie można wykonywać modularnie:
  $a^j = a^{j \mod |G|}$
  – jeśli $NWD(j, |G|) = 1$, to $f(a) = a^j$ jest bijekcją, odwrotną jest $g(a) = a^i$, gdzie $j \cdot i = 1 \mod |G|$

Twierdzenie Fermata (małe)

- Tw.: jeśli p jest liczbą pierwszą i nie dzieli a, to $a^{p-1} = 1 \mod p$
- Dw.: $a \mod p$ jest elementem $\mathbb{Z}_p^*$ (tzn. $\{1, 2, \ldots, p-1\}$), $|\mathbb{Z}_p| = p - 1$ i stosujemy poprzednie twierdzenie
- przykład: $2^{10} = 1 \mod 11$
  stąd $2^{123456789} = 2^9 = 6 \mod 11$
- $a^{560} = a^0 = 1 \mod 3$ ponieważ $560 = 0 \mod 2$
  $a^{560} = a^0 = 1 \mod 11$ ponieważ $560 = 0 \mod 10$
  $a^{560} = a^0 = 1 \mod 17$ ponieważ $560 = 0 \mod 16$
  więc $a^{560} = 1 \mod 561$ (chińskie tw. o resztach, $561 = 3 \cdot 11 \cdot 17$)
- test pierwszości: szybkie potęgowanie w celu sprawdzenia czy $a^{n-1} = 1 \mod n$, dla różnych wartości a
  – jeśli nie ma równości, to liczba nie jest pierwsza
  – 561 jest wyjątkiem, dowolne a spełnia $a^{560} = 1 \mod 561$

Funkcja Eulera φ

- $\varphi(n) =$ liczba liczb $a \in \{1, .., n-1\}$ takich że $NWD(a, n) = 1$
- tw. Euklidesa: istnieją współczynniki k, ℓ takie, że $k \cdot a + \ell \cdot n = NWD(a, n)$
- czyli $\varphi(n)$ jest rzędem grupy multiplikatywnej $\mathbb{Z}_n^*$
  – jeśli $n = p$, to $\varphi(p) = p - 1$ (tw. Fermata)
  – jeśli $n = p^k$, to $\varphi(p^k) = p^k - p^{k-1} = (1 - \frac{1}{p}) \cdot n$
  (nie są względnie pierwsze wielokrotności p: $\left\{p, 2 \cdot p, \ldots, p^k - p\right\}$)
  – ogólnie $\varphi(n) = n \cdot$ iloczyn $(1 - \frac{1}{p})$ po wszystkich dzielnikach pierwszych n (chińskie tw. o resztach)
  – ważny przypadek $\varphi(p \cdot q) = (p - 1) \cdot (q - 1)$
  – np. $\varphi(26) = \varphi(2 \cdot 13) = 12$

Twierdzenie Eulera

- Tw.: Jeśli $NWD(a, n) = 1$, to $a^{\varphi(n)} = 1 \mod n$
- małe tw. Fermata jest przypadkiem szczególnym
- Wniosek: jeśli $NWD(a, n) = 1$, $x = y \mod \varphi(n)$, to $a^x = a^y \mod n$
  – tzn. działania mod n na potęgach można zastąpić działaniami mod $\varphi(n)$ w wykładniku
  – przykład: $2^{43210} = 2^{10} = 10 \mod 26$, bo $\varphi(26) = 12$, $43210 = 10 \mod 12$ oraz $2^{10} = 1024 = 10 \mod 26$
  – albo: $3^{456789} = 3^9 = 1 \mod 26$, bo $456789 = 9 \mod 12$ oraz $3^9 = 19683 = 1 \mod 26$ (oczywiście nie liczymy 9. potęgi tylko szybkie potęgowanie)