Matematyka dyskretna

Wykład 11: Kryptografia z kluczem publicznym

Gniewomir Sarbicki

Idea kryptografii z kluczem publicznym:

$$\text{wiadomość} \xrightarrow{f} \text{szyfrogram} \xrightarrow{f^{-1}} \text{wiadomość}$$

Funkcja f (klucz publiczny) jest znana publicznie, a jej odwrotność f^{-1} (klucz prywatny) jest znana tylko właścicielowi klucza. Każdy może zakodować wiadomość, którą będzie mógł przeczytać tylko właściciel klucza.

Żeby to było możliwe, wyznaczenie f^{-1} na podstawie f musi być niemożliwe (lub beznadziejnie trudne). Jakie znamy takie funkcje?

- funkcja wykładnicza (El-Gamal)
- wymnożenie dwóch czynników pierwszych (RSA)

Kryptosystem El-Gamal

Odbiorca wybiera liczbę pierwszą p i jeden z jej pierwiastków pierwotnych B (gwarantuje to różnowartościowość funkcji $k \to B^k$).

Następnie wybiera pewien wykładnik m jako swój klucz prywatny i oblicza $C = B^m$. Jako klucz publiczny ujawnia trójkę $[p, B, C]$.

Nadawca by przesłać blok wiadomości P wybiera dowolną liczbę $r \in \{2, \ldots, p-1\}$ i na podstawie klucza publicznego generuje dwa bloki szyfrogramu:

$$X_1 = B^r, \quad X_2 = P \cdot C^r \quad (\bmod p)$$

Odbiorca wykonuje operację deszyfrującą z użyciem klucza prywatnego: $P = X_2 \cdot X_1^{p-1-m} (\bmod p)$

Kryptosystem El-Gamal

Dowód:

$$\begin{aligned} X_2 \cdot X_1^{p-1-m} &= P \cdot C^r \cdot (B^r)^{p-1-m} \\ &= P \cdot B^{mr} B^{r(p-1)-rm} \\ &= P \cdot B^{(p-1)r} = P \cdot 1^r = P \end{aligned}$$

Przedostatnia równość z twierdzenia Fermata.

Żeby obliczyć klucz prywatny z publicznego, trzeba umieć obliczyć $log_B(C)$ w $\mathbb{Z}_p$.

Kryptosystem El-Gamal

Przykład: Kodujemy litery alfabetu, które można zapisywać w 5-cio bitowych blokach. Z przedziału $2^5, 2^6$ wybieramy liczbę pierwszą $p = 41$.

Weźmy: $B = 13, m = 29$. Obliczamy $C = B^m = 34$. Dla klucza prywatnego $m = 29$ wygenerowaliśmy klucz publiczny $[p = 41, B = 13, C = 34]$.

Nadawca chce nam wysłać tekst WITAJ, zapisany jako numery liter w alfabecie: $[22, 8, 19, 0, 9]$.

Nadawca dla każdej litery losuje liczbę r i tworzy szyfrogram wykorzystując wzór $(X_1, X_2) = (B^r, P \cdot C^r)$.

Odbiorca dekoduje szyfrogram wzorem $X_2 \cdot X_1^{p-1-m}$

Kryptosystem El-Gamal

```
$ python3
>>> from random import randint
>>> p=41
>>> B=13
>>> f = lambda x:B**x % p        # definiujemy f.wykladnicza o podst B w ciele Z_p
>>> m=29                         # wybieramy klucz prywatny
>>> C = f(m)
>>> C
34
>>> tekst = [22,8,19,0,9]
>>> pary = [(t,randint(0,p-1)) for t in tekst]          # nadawca generuje losowe r
>>> pary                                                # dla kazdego bloku tekstu
[(22, 11), (8, 3), (19, 39), (0, 19), (9, 16)]
>>> szyfrogram = [(B**r % p,P*C**r % p) for P,r in pary]        # szyfrowanie
>>> szyfrogram
[(37, 15), (14, 11), (8, 13), (1, 0), (4, 33)]
>>> tekst = [s[1]*s[0]**(p-1-m) % p for s in szyfrogram]        # deszyfrowanie
>>> tekst
[22, 8, 19, 0, 9]
>>> exit()
```

Podpis elektroniczny w systemie El-Gamal

Podpisujący wybiera dowolne $r : NWD(r, p-1) = 1$ i oblicza (na podstawie klucza prywatnego) dwie liczby u i v:

$$u = B^r, \qquad rv + mu = P \mod p-1$$

Wysyła je do odbiorcy wraz z blokiem P, który jest teraz podpisany. Odbiorca na podstawie klucza publicznego sprawdza, czy:

$$C^u u^v = B^P \mod p$$

Jeżeli to prawda, to znaczy że wiarygodność bloku P potwierdził ktoś kto zna klucz prywatny.

Dowód:

$$C^u u^v = B^{mu} \cdot B^{rv} = B^{mu+rv} = B^{P(+\alpha\cdot(p-1))} = B^P \cdot (B^{p-1})^\alpha = B^P$$

Podpis elektroniczny w systemie El-Gamal

Przykład: Chcemy podpisać blok $P = 18$. Kluczem publicznym jest $[p = 41, B = 13, C = 34]$, a prywatnym $m = 29$ (jak poprzednio).

Wybieramy $r = 7$. Obliczamy:

$$u = B^r \mod p = 13^7 \mod 41 = 26$$
$$v = r^{-1}(P - mu) \mod p - 1 = 23 \cdot (18 - 29 \cdot 10) = 32$$

i wysyłamy to jako podpis bloku P.

Odbiorca na podstawie klucza publicznego oblicza liczby:

$$C^u u^v = 34^{26} \cdot 26^{32} \mod 41 = 8$$
$$B^P = 13^{18} \mod 41 = 8$$

zatem wiadomość wysłał posiadacz klucza prywatnego który odpowiada kluczowi publicznemu!

Podpis elektroniczny w systemie El-Gamal

```
$ python3
>>> p=41; B=13; C=34          # nasz klucz publiczny
>>> m=29                      # i prywatny
>>> P=18                      # blok ktory podpisujemy
>>> r=7                       # wybieramy r
>>> u=B**r % p
>>> u
26
>>> v = (P-m*u)*r**(16-1) % (p - 1)      # r^-1 = r^(phi(p-1)-1)
>>> v
32
>>> C**u*u**v % p
8
>>> B**P % p
8
>>> exit()
```

Kryptosystem RSA

Wybieramy dwie duże liczby pierwsze (ale niezbyt bliskie sobie) p i q. Tworzymy liczbę złożoną $n = pq$ i wybieramy $e \in \mathbb{Z}_n$ taki, że $NWD(e, \phi(n)) = 1$. Istnieje wtedy takie d, że $ed = 1 \mod \phi(n)$.

Para (n, e) jest kluczem publicznym, a d kluczem prywatnym. Blok wiadomości b kodujemy jako $c = b^e (\text{mod } pq)$,
a dekodujemy jako $b = c^d (\text{mod } pq)$.

Dowód: Musimy udowodnić, że dla dowolnego b:
$b^{ed} = b \mod pq \iff b^{ed-1} = 1.$

$ed - 1 = h(p-1)(q-1)$. Rozważamy dwa przypadki:
gdy $b = 0 \mod p$, gdy $b \neq 0 \mod p$.

W pierwszym przypadku $b^{ed} = 0^{ed} = b \mod p$. W drugim przypadku $NWD(b, p) = 1$ i z twierdzenia Fermata $b^{p-1} = 1 \mod p \implies b^{ed-1} = 1 \mod p$, zatem $b^{ed} = b \mod p$.

Tak samo udowodnimy, że $b^{ed} = b \mod q$, zatem z ChToR:
$b^{ed} = b \mod pq$ $\square$

Kryptosystem RSA

Przykład: Weźmy dwie liczby pierwsze $p = 11$ i $q = 13$. Wtedy $n = 143$ i $\phi(n) = 120$.

Weźmy $e = 7$ - jest wzgl. pierwsze ze 120. $d = e^{-1} \mod 120 = e^{\phi(\phi(n))-1} = 7^{31} \mod 120 = 103$.

Niech wiadomością będzie liczba 58. Po zakodowaniu: $58^7 \mod 143 = 20$

Dekodujemy kluczem prywatnym: $20^{103} = 58$

Kryptosystem RSA

```
$ python3
>>> p=11;q=13;n=p*q;phi=(p-1)*(q-1)
>>> p,q,n,phi
11 13 143 120
>>> e=7                    # wybieramy liczbe wzglednie pierwsza z phi (klucz publiczny)
>>> d=e**(32-1) % phi  # liczymy jej odwrotnosc w Z_phi (klucz prywatny)
>>> d
103
>>> x=58**e % n            # kodujemy wiadomosc
>>> x
20
>>> x ** d % n           # dekodujemy wiadomosc
58
>>> exit()
```

Podpis elektroniczny w systemie RSA

Nadawca koduje blok b swoim kluczem prywatnym: b^d i wysyła do odbiorcy oba bloki $[b, b^d]$.

Odbiorca dekoduje drugi blok używając wykładnika e z klucza publicznego: $(b^d)^e$. Jeżeli w wyniku wyszło b, to znaczy że wiadomość podpisał posiadacz klucza prywatnego.