

Teoria kodowania - metody Rabina i RSA

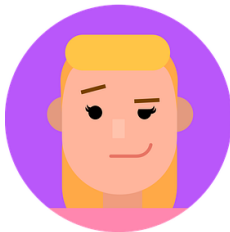
Aleksandra Gorzkowska

Elektronika i Telekomunikacja
Wydział Informatyki, Elektroniki i Telekomunikacji

Kryptografia z kluczem publicznym



Kryptografia z kluczem publicznym



Alicja i Bob postępują według następującego protokołu:

Alicja i Bob postępują według następującego protokołu:

- 1 Bob generuje funkcję szyfrującą E oraz funkcję deszyfrującą D ,
takie że $D(E(I)) = I$, gdzie I to dowolna wiadomość,

Alicja i Bob postępują według następującego protokołu:

- 1 Bob generuje funkcję szyfrującą E oraz funkcję deszyfrującą D , takie że $D(E(I)) = I$, gdzie I to dowolna wiadomość,
- 2 Bob przesyła jawnie funkcję E do Alicji (Ewa również poznaje funkcję E),

Alicja i Bob postępują według następującego protokołu:

- 1 Bob generuje funkcję szyfrującą E oraz funkcję deszyfrującą D , takie że $D(E(I)) = I$, gdzie I to dowolna wiadomość,
- 2 Bob przesyła jawnie funkcję E do Alicji (Ewa również poznaje funkcję E),
- 3 Alicja szyfruje wiadomość używając funkcji E : $m = E(I)$,

Alicja i Bob postępują według następującego protokołu:

- 1 Bob generuje funkcję szyfrującą E oraz funkcję deszyfrującą D , takie że $D(E(I)) = I$, gdzie I to dowolna wiadomość,
- 2 Bob przesyła jawnie funkcję E do Alicji (Ewa również poznaje funkcję E),
- 3 Alicja szyfruje wiadomość używając funkcji E : $m = E(I)$,
- 4 Alicja przesyła jawnie do Boba zaszyfrowaną wiadomość m (Ewa widzi ten przekaz),

Alicja i Bob postępują według następującego protokołu:

- 1 Bob generuje funkcję szyfrującą E oraz funkcję deszyfrującą D , takie że $D(E(I)) = I$, gdzie I to dowolna wiadomość,
- 2 Bob przesyła jawnie funkcję E do Alicji (Ewa również poznaje funkcję E),
- 3 Alicja szyfruje wiadomość używając funkcji E : $m = E(I)$,
- 4 Alicja przesyła jawnie do Boba zaszyfrowaną wiadomość m (Ewa widzi ten przekaz),
- 5 Bob odszyfrowuje wiadomość używając funkcji D , czyli znajduje $I = D(m)$.

Alicja i Bob postępują według następującego protokołu:

- 1 Bob generuje funkcję szyfrującą E oraz funkcję deszyfrującą D , takie że $D(E(I)) = I$, gdzie I to dowolna wiadomość,
- 2 Bob przesyła jawnie funkcję E do Alicji (Ewa również poznaje funkcję E),
- 3 Alicja szyfruje wiadomość używając funkcji E : $m = E(I)$,
- 4 Alicja przesyła jawnie do Boba zaszyfrowaną wiadomość m (Ewa widzi ten przekaz),
- 5 Bob odszyfrowuje wiadomość używając funkcji D , czyli znajduje $I = D(m)$.

Funkcję E nazywamy **kluczem publicznym**. Funkcję D nazywamy **kluczem prywatnym**.

Alicja i Bob postępują według następującego protokołu:

- 1 Bob generuje funkcję szyfrującą E oraz funkcję deszyfrującą D , takie że $D(E(I)) = I$, gdzie I to dowolna wiadomość,
- 2 Bob przesyła jawnie funkcję E do Alicji (Ewa również poznaje funkcję E),
- 3 Alicja szyfruje wiadomość używając funkcji E : $m = E(I)$,
- 4 Alicja przesyła jawnie do Boba zaszyfrowaną wiadomość m (Ewa widzi ten przekaz),
- 5 Bob odszyfrowuje wiadomość używając funkcji D , czyli znajduje $I = D(m)$.

Funkcję E nazywamy **kluczem publicznym**. Funkcję D nazywamy **kluczem prywatnym**.

Jeśli tym razem Bob chce przesłać wiadomość do Alicji, to Alicja generuje swoje funkcje E' i D' i w sposób jawny udostępnia funkcję E' Bobowi.

Każdą wiadomość tekstową, która ma zostać w ten sposób przesłana można zamienić na liczbę. Np. używając powszechnie znanego kodu ASCII.

Każdą wiadomość tekstową, która ma zostać w ten sposób przesłana można zamienić na liczbę. Np. używając powszechnie znanego kodu ASCII.

Jak jednak znaleźć funkcje E i D ? Podanie do wiadomości publicznej funkcji E może skutkować jej "odwróceniem" i tym samym znalezieniem funkcji D . **Chcemy tego uniknąć!**

Metoda Rabina

Szyfrowana liczba: l

Klucz publiczny: liczba n ; funkcja szyfrująca $E(l) = l^2 \pmod{n}$

Przy czym $l < n$ oraz $n = p \cdot q$, gdzie $p, q \in \mathbb{P}$, $p, q \equiv 3 \pmod{4}$.

Metoda Rabina

Szyfrowana liczba: l

Klucz publiczny: liczba n ; funkcja szyfrująca $E(l) = l^2 \pmod{n}$

Przy czym $l < n$ oraz $n = p \cdot q$, gdzie $p, q \in \mathbb{P}$, $p, q \equiv 3 \pmod{4}$.

Alicja prześle więc Bobowi liczbę $m = l^2 \pmod{n}$.

Metoda Rabina

Szyfrowana liczba: l

Klucz publiczny: liczba n ; funkcja szyfrująca $E(l) = l^2 \pmod{n}$

Przy czym $l < n$ oraz $n = p \cdot q$, gdzie $p, q \in \mathbb{P}$, $p, q \equiv 3 \pmod{4}$.

Alicja prześle więc Bobowi liczbę $m = l^2 \pmod{n}$.

Dlaczego Ewa nie może teraz po prostu obliczyć pierwiastka z liczby m ? Jest to pierwiastek w $\mathbb{Z}_n$.

Metoda Rabina

Szyfrowana liczba: l

Klucz publiczny: liczba n ; funkcja szyfrująca $E(l) = l^2 \pmod{n}$

Przy czym $l < n$ oraz $n = p \cdot q$, gdzie $p, q \in \mathbb{P}$, $p, q \equiv 3 \pmod{4}$.

Alicja prześle więc Bobowi liczbę $m = l^2 \pmod{n}$.

Dlaczego Ewa nie może teraz po prostu obliczyć pierwiastka z liczby m ? Jest to pierwiastek w $\mathbb{Z}_n$.

Przykład

$n = 13$, $m = 10$

Używając zwykłego kalkulatora, otrzymamy wynik

$\sqrt{10} = 3,1612\dots$

Nie jest to jednak przekazywana wiadomość.

Obliczamy $\sqrt{10}$ w $\mathbb{Z}_{13}$: $6^2 = 36 = 10 \pmod{13}$,

$7^2 = 49 = 10 \pmod{13}$.

Zaszyfrowaną wiadomością była więc liczba 6 lub 7.

Uwaga

Jeśli $b^2 = a \pmod{n}$, to także $(-b)^2 = a \pmod{n}$.

Uwaga

Jeśli $b^2 = a \pmod{n}$, to także $(-b)^2 = a \pmod{n}$.

Przeliczmy: $(n - b)^2 = n^2 - 2nb + b^2 = b^2 \pmod{n} = a \pmod{n}$.

Uwaga

Jeśli $b^2 = a \pmod{n}$, to także $(-b)^2 = a \pmod{n}$.

Przeliczmy: $(n - b)^2 = n^2 - 2nb + b^2 = b^2 \pmod{n} = a \pmod{n}$.

Definicja

Niech $n \in \mathbb{N}_+$, $a \in \mathbb{Z}_n$. Mówimy, że liczba a jest **residuum kwadratowym** modylo n , jeśli istnieje $b \in \mathbb{Z}_n$, takie że $a = b^2 \pmod{n}$.

Twierdzenie

Niech $p \in \mathbb{P}$, $a \in \mathbb{Z}_p \setminus \{0\}$. Jeśli a jest residuum kwadratowym, to a ma dokładnie dwa pierwiastki kwadratowe w $\mathbb{Z}_p$.

Twierdzenie

Niech $p \in \mathbb{P}$, $a \in \mathbb{Z}_p \setminus \{0\}$. Jeśli a jest residuum kwadratowym, to a ma dokładnie dwa pierwiastki kwadratowe w $\mathbb{Z}_p$.

Twierdzenie

Niech $p \in \mathbb{P}$, $p \equiv 3 \pmod{4}$. Jeśli a jest residuum kwadratowym, to pierwiastki kwadratowe z a w $\mathbb{Z}_p$ mają postać $a^{\frac{p+1}{4}} \pmod{p}$ oraz $-a^{\frac{p+1}{4}} \pmod{p}$.

Twierdzenie

Niech $p \in \mathbb{P}$, $a \in \mathbb{Z}_p \setminus \{0\}$. Jeśli a jest residuum kwadratowym, to a ma dokładnie dwa pierwiastki kwadratowe w $\mathbb{Z}_p$.

Twierdzenie

Niech $p \in \mathbb{P}$, $p \equiv 3 \pmod{4}$. Jeśli a jest residuum kwadratowym, to pierwiastki kwadratowe z a w $\mathbb{Z}_p$ mają postać $a^{\frac{p+1}{4}} \pmod{p}$ oraz $-a^{\frac{p+1}{4}} \pmod{p}$.

Dowód.

Niech $a = b^2 \pmod{p}$. Korzystając z twierdzenia Eulera dla liczb b oraz p , mamy $a^{\frac{p-1}{2}} = b^{p-1} = 1 \pmod{p}$.

Przeliczmy: $\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}+1} = a \pmod{p}$.



Alicja przesyła jawnie liczbę $m = E(l) = l^2 \pmod{n}$, gdzie $n = p \cdot q$,
 $p, q \equiv 3 \pmod{4}$.

Alicja przesyła jawnie liczbę $m = E(l) = l^2 \pmod{n}$, gdzie $n = p \cdot q$,
 $p, q \equiv 3 \pmod{4}$.

Bob oblicza pierwiastki kwadratowe modulo p oraz q z liczby m :

$$x_1 = m^{\frac{p+1}{4}} \pmod{p}, \quad x_2 = -m^{\frac{p+1}{4}} \pmod{p}, \quad x_3 = m^{\frac{q+1}{4}} \pmod{q}, \\ x_4 = -m^{\frac{q+1}{4}} \pmod{q}.$$

Alicja przesyła jawnie liczbę $m = E(l) = l^2 \pmod{n}$, gdzie $n = p \cdot q$, $p, q \equiv 3 \pmod{4}$.

Bob oblicza pierwiastki kwadratowe modulo p oraz q z liczby m :

$$x_1 = m^{\frac{p+1}{4}} \pmod{p}, \quad x_2 = -m^{\frac{p+1}{4}} \pmod{p}, \quad x_3 = m^{\frac{q+1}{4}} \pmod{q}, \\ x_4 = -m^{\frac{q+1}{4}} \pmod{q}.$$

A następnie rozwiązuje cztery układy kongruencji.

$$\begin{cases} l = x_1 \pmod{p} \\ l = x_3 \pmod{q} \end{cases} \quad \begin{cases} l = x_2 \pmod{p} \\ l = x_3 \pmod{q} \end{cases}$$

$$\begin{cases} l = x_1 \pmod{p} \\ l = x_4 \pmod{q} \end{cases} \quad \begin{cases} l = x_2 \pmod{p} \\ l = x_4 \pmod{q} \end{cases}$$

Każdy z tych układów ma jednoznaczne rozwiązanie modulo $p \cdot q$. Wynika to z chińskiego twierdzenia o resztach. Otrzymujemy cztery rozwiązania w postaci liczb modulo $n = p \cdot q$,

Każdy z tych układów ma jednoznaczne rozwiązanie modulo $p \cdot q$. Wynika to z chińskiego twierdzenia o resztach. Otrzymujemy cztery rozwiązania w postaci liczb modulo $n = p \cdot q$,

Liczby te zamieniamy w wiadomość tekstową (posługując się np. kodem ASCII) i wybieramy jedyną sensowną spośród tych wiadomości.

Przykład

$$n = 253 = 11 \cdot 23, A = 65 = I$$

Metoda RSA

Nazwa metody pochodzi od pierwszych liter nazwisk jej twórców:
Rivest, Szamir i Adleman.

Opis metody:

Metoda RSA

Nazwa metody pochodzi od pierwszych liter nazwisk jej twórców: Rivest, Szamir i Adleman.

Opis metody:

- 1 Bob znajduje dwie duże liczby pierwsze p oraz q . Oblicza $n = p \cdot q$ oraz $\varphi(n) = (p - 1)(q - 1)$. Wybiera dowolną liczbę $e \in \mathbb{Z}_{\varphi(n)}^*$,

Metoda RSA

Nazwa metody pochodzi od pierwszych liter nazwisk jej twórców: Rivest, Szamir i Adleman.

Opis metody:

- 1 Bob znajduje dwie duże liczby pierwsze p oraz q . Oblicza $n = p \cdot q$ oraz $\varphi(n) = (p - 1)(q - 1)$. Wybiera dowolną liczbę $e \in \mathbb{Z}_{\varphi(n)}^*$,
- 2 Bob przesyła Alicji **klucz publiczny**: liczby n i e ,

Metoda RSA

Nazwa metody pochodzi od pierwszych liter nazwisk jej twórców: Rivest, Szamir i Adleman.

Opis metody:

- 1 Bob znajduje dwie duże liczby pierwsze p oraz q . Oblicza $n = p \cdot q$ oraz $\varphi(n) = (p - 1)(q - 1)$. Wybiera dowolną liczbę $e \in \mathbb{Z}_{\varphi(n)}^*$,
- 2 Bob przesyła Alicji **klucz publiczny**: liczby n i e ,
- 3 Alicja liczy i przesyła Bobowi liczbę $m = l^e \pmod{n}$, przy czym $l < n$,

Metoda RSA

Nazwa metody pochodzi od pierwszych liter nazwisk jej twórców: Rivest, Szamir i Adleman.

Opis metody:

- 1 Bob znajduje dwie duże liczby pierwsze p oraz q . Oblicza $n = p \cdot q$ oraz $\varphi(n) = (p - 1)(q - 1)$. Wybiera dowolną liczbę $e \in \mathbb{Z}_{\varphi(n)}^*$,
- 2 Bob przesyła Alicji **klucz publiczny**: liczby n i e ,
- 3 Alicja liczy i przesyła Bobowi liczbę $m = l^e \pmod{n}$, przy czym $l < n$,
- 4 Bob oblicza $d = e^{-1} \pmod{\varphi(n)}$ i deszyfruje wiadomość

$$l = m^d = (l^e)^d \pmod{n}.$$

Przykład

$$n = 629 = 17 \cdot 37, e = 7, l = 5$$

Dlaczego to działa?

Dlaczego to działa?

Chcemy pokazać, że $m^d = 1 \pmod{n}$.

Skoro $d = e^{-1} \pmod{\varphi(n)}$, to $ed = 1 \pmod{\varphi(n)}$, czyli $ed = 1 + k\varphi(n)$, dla pewnego $k \in \mathbb{Z}$.

Dlaczego to działa?

Chcemy pokazać, że $m^d = l \pmod{n}$.

Skoro $d = e^{-1} \pmod{\varphi(n)}$, to $ed = 1 \pmod{\varphi(n)}$, czyli $ed = 1 + k\varphi(n)$, dla pewnego $k \in \mathbb{Z}$.

Przypadek I: $l \perp n$.

Korzystając z twierdzenia Eulera dla liczb l i n , mamy:

$$m^d = (l^e)^d = l^{1+k\varphi(n)} = l \cdot (l^{\varphi(n)})^k = l \cdot 1^k = l \pmod{n}.$$

Przypadek II: $l \nmid n$.

Wtedy albo $p|l$, albo $q|l$ (gdyby oba warunki zachodziły jednocześnie, to l byłoby wielokrotnością n . A zakładamy, że $l < n$). Bez straty ogólności $p|l$ oraz $q \nmid l$. Stąd $q \perp l$ i korzystając z twierdzenia Eulera dla liczb l i q mamy:

$$l^{ed} = l^{1+k(p-1)(q-1)} = l \cdot (l^{q-1})^{k(p-1)} = l \cdot 1^{k(p-1)} \pmod{q}.$$

Skoro $p|l$, to $l = 0 \pmod{p}$. Otrzymujemy układ kongruencji:

$$\begin{cases} l = 0 \pmod{p} \\ l = m^d \pmod{q} \end{cases}$$

Z chińskiego twierdzenia o resztach wiemy, że l jest jedynym rozwiązaniem tego układu modulo $n = p \cdot q$.