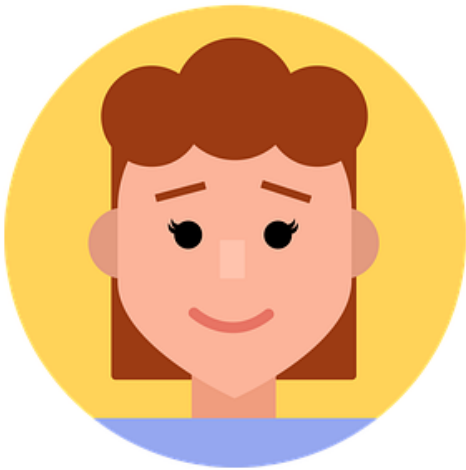
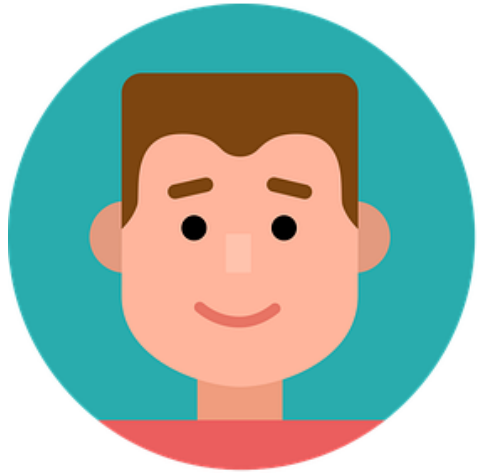
Teoria kodowania - metody Rabina i RSA

Aleksandra Gorzkowska

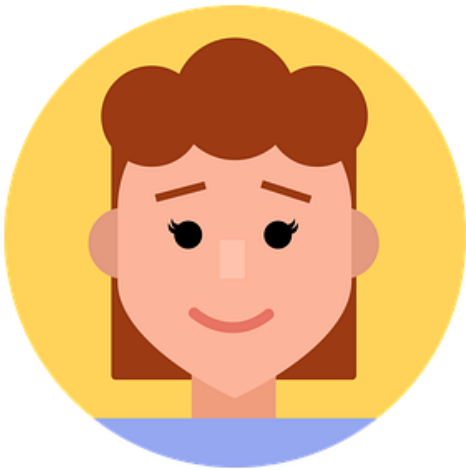
Elektronika i Telekomunikacja
Wydział Informatyki, Elektroniki i Telekomunikacji

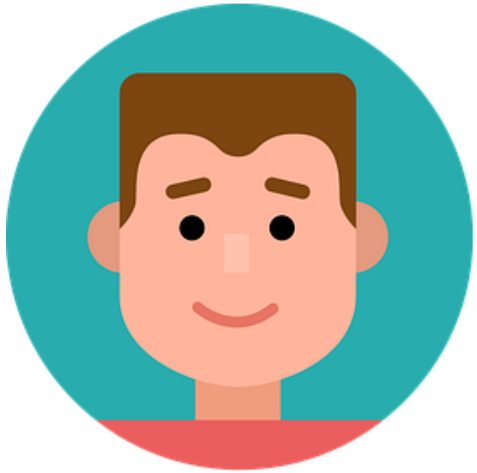
Kryptografia z kluczem publicznym

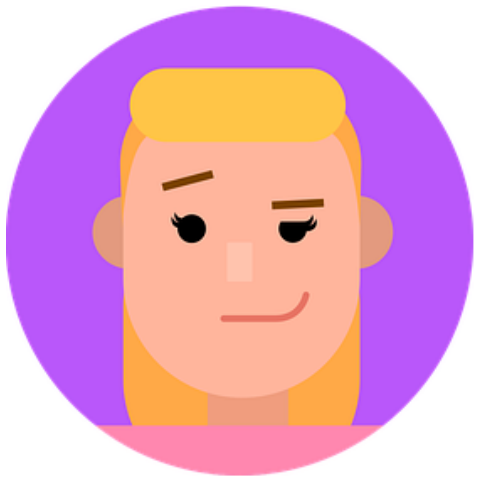




Kryptografia z kluczem publicznym







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!

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!

Omówimy dwie metody szyfrowania z kluczem publicznym. Obie opierają się na fakcie, że rozkład dużych liczb na czynniki pierwsze jest niezwykle trudny i czasochłonny, nawet dla komputera. To właśnie skutecznie uniemożliwia znalezienie funkcji D podsłuchiwaczom.

Metoda Rabina

Szyfrowana liczba: l

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

Przy czym $l < n$ oraz $n = p \cdot q$, gdzie $p, q \in \mathbb{P}$, $p, q = 3 (\mathrm{mod}\ 4)$.

Metoda Rabina

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

Przy czym $l < n$ oraz $n = p \cdot q$, gdzie $p, q \in \mathbb{P}$, $p, q = 3 (\mathrm{mod}\ 4)$.

Alicja prześle więc Bobowi liczbę $m = l^2 (\mathrm{mod}\ n)$.

Metoda Rabina

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

Przy czym $l < n$ oraz $n = p \cdot q$, gdzie $p, q \in \mathbb{P}$, $p, q = 3 (\mathrm{mod}\ 4)$.

Alicja prześle więc Bobowi liczbę $m = l^2 (\mathrm{mod}\ n)$.
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 $E(l) = l^2 (\mathrm{mod}\ n)$

Przy czym $l < n$ oraz $n = p \cdot q$, gdzie $p, q \in \mathbb{P}$, $p, q = 3 (\mathrm{mod}\ 4)$.

Alicja prześle więc Bobowi liczbę $m = l^2 (\mathrm{mod}\ n)$.
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
$\sqrt{10} = 3,1612....$
Nie jest to jednak przekazywana wiadomość.
Obliczamy $\sqrt{10}$ w $\mathbb{Z}_{13}$: $6^2 = 36 = 10 (\mathrm{mod}\ 13)$,
$7^2 = 49 = 10 (\mathrm{mod}\ 13)$.
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 $p \in \mathbb{P}$, $p = 3 (\mathrm{mod}\ 4)$. Jeśli a jest residuum kwadratowym, to pierwiastki kwadratowe z a w $\mathbb{Z}_p$ mają postać $a^{\frac{p+1}{4}} (\mathrm{mod}\ p)$ oraz $-a^{\frac{p+1}{4}} (\mathrm{mod}\ p)$.

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

Dowód.

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

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

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

Alicja przesyła jawnie liczbę $m = E(I) = I^2 (\mathrm{mod}\ n)$, gdzie $n = p \cdot q$, $p, q = 3 (\mathrm{mod}\ 4)$.
Bob oblicza pierwiastki kwadratowe modulo p oraz q z liczby m: $x_1 = m^{\frac{p+1}{4}} (\mathrm{mod}\ p)$, $x_2 = -m^{\frac{p+1}{4}} (\mathrm{mod}\ p)$, $x_3 = m^{\frac{q+1}{4}} (\mathrm{mod}\ q)$, $x_4 = -m^{\frac{q+1}{4}} (\mathrm{mod}\ q)$.

Alicja przesyła jawnie liczbę $m = E(l) = l^2 (\mathrm{mod}\ n)$, gdzie $n = p \cdot q$, $p, q = 3 (\mathrm{mod}\ 4)$.
Bob oblicza pierwiastki kwadratowe modulo p oraz q z liczby m: $x_1 = m^{\frac{p+1}{4}} (\mathrm{mod}\ p)$, $x_2 = -m^{\frac{p+1}{4}} (\mathrm{mod}\ p)$, $x_3 = m^{\frac{q+1}{4}} (\mathrm{mod}\ q)$, $x_4 = -m^{\frac{q+1}{4}} (\mathrm{mod}\ q)$.
A następnie rozwiązuje cztery układy kongruencji.

$$\begin{cases} l = x_1 (\mathrm{mod}\ p) \\ l = x_3 (\mathrm{mod}\ q) \end{cases} \qquad \begin{cases} l = x_2 (\mathrm{mod}\ p) \\ l = x_3 (\mathrm{mod}\ q) \end{cases}$$

$$\begin{cases} l = x_1 (\mathrm{mod}\ p) \\ l = x_4 (\mathrm{mod}\ q) \end{cases} \qquad \begin{cases} l = x_2 (\mathrm{mod}\ p) \\ l = x_4 (\mathrm{mod}\ q) \end{cases}$$

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:

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 $m = l^e (\mathrm{mod}\ n)$, przy czym $l < n$,
4. Bob oblicza $d = e^{-1} (\mathrm{mod}\ \varphi(n))$ i deszyfruje wiadomość

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

Przykład

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

Dlaczego to działa?

Dlaczego to działa?

Chcemy pokazać, że $m^d = l (\mathrm{mod}\ n)$.

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

Dlaczego to działa?

Chcemy pokazać, że $m^d = l (\mathrm{mod}\ n)$.

Skoro $d = e^{-1} (\mathrm{mod}\ \varphi(n))$, to $ed = 1 (\mathrm{mod}\ \varphi(n))$, 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:
$m^d = (l^e)^d = l^{1+k\varphi(n)} = l \cdot (l^{\varphi(n)})^k = l \cdot 1^k = l (\mathrm{mod}\ n)$.

Przypadek II: $l \not\perp n$.
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:

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

Skoro $p|l$, to $l = 0(\mathrm{mod}\ p)$. Otrzymujemy układ kongruencji:

$$\begin{cases} l &= 0(\mathrm{mod}\ p) \\ l &= m^d(\mathrm{mod}\ q) \end{cases}$$

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