# Kryptografia

## z elementami kryptografii kwantowej

**Ryszard Tanaś**

http://zon8.physd.amu.edu.pl/~tanas

**Wykład 5**

# Spis treści

# 9 Algorytmy asymetryczne — RSA

- Witfield Diffie i Martin Hellman — idea kryptografii z kluczem publicznym, rok 1976
- RSA — Ron Rivest, Adi Shamir i Leonard Adleman, rok 1978
- bezpieczeństwo algorytmu RSA opiera się na trudności obliczeniowej związanej z rozkładem dużych liczb na czynniki (faktoryzacja)

# 9 Algorytmy asymetryczne — RSA

- Witfield Diffie i Martin Hellman — idea kryptografii z kluczem publicznym, rok 1976
- RSA — Ron Rivest, Adi Shamir i Leonard Adleman, rok 1978
- bezpieczeństwo algorytmu RSA opiera się na trudności obliczeniowej związanej z rozkładem dużych liczb na czynniki (faktoryzacja)

# 9 Algorytmy asymetryczne — RSA

- Witfield Diffie i Martin Hellman — idea kryptografii z kluczem publicznym, rok 1976
- RSA — Ron Rivest, Adi Shamir i Leonard Adleman, rok 1978
- bezpieczeństwo algorytmu RSA opiera się na trudności obliczeniowej związanej z rozkładem dużych liczb na czynniki (faktoryzacja)

# 9 Algorytmy asymetryczne — RSA

- Witfield Diffie i Martin Hellman — idea kryptografii z kluczem publicznym, rok 1976
- RSA — Ron Rivest, Adi Shamir i Leonard Adleman, rok 1978
- bezpieczeństwo algorytmu RSA opiera się na trudności obliczeniowej związanej z rozkładem dużych liczb na czynniki (faktoryzacja)

## 9.1 Algorytm RSA

- Wybieramy dwie duże liczby pierwsze: $\{p, q\}$
- Obliczamy ich iloczyn (łatwo): $n = pq$
- Wybieramy losowo liczbę $e < n$
  względnie pierwszą z liczbą $(p-1)(q-1)$
- Liczba $e$ będzie kluczem szyfrującym
- Znajdujemy liczbę $d$ taką, że
  $ed \equiv 1 \pmod{(p-1)(q-1)}$
- lub inaczej
  $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
- Liczby $d$ i $n$ są także względnie pierwsze

## 9.1 Algorytm RSA

- Wybieramy dwie duże liczby pierwsze: $\{p, q\}$
- Obliczamy ich iloczyn (łatwo): $n = pq$
- Wybieramy losowo liczbę $e < n$ względnie pierwszą z liczbą $(p-1)(q-1)$
- Liczba $e$ będzie kluczem szyfrującym
- Znajdujemy liczbę $d$ taką, że $ed \equiv 1 \pmod{(p-1)(q-1)}$
- lub inaczej $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
- Liczby $d$ i $n$ są także względnie pierwsze

## 9.1 Algorytm RSA

- Wybieramy dwie duże liczby pierwsze: $\{p, q\}$
- Obliczamy ich iloczyn (łatwo): $n = pq$
- Wybieramy losowo liczbę $e < n$
  względnie pierwszą z liczbą $(p-1)(q-1)$
- Liczba $e$ będzie kluczem szyfrującym
- Znajdujemy liczbę $d$ taką, że
  $ed \equiv 1 \pmod{(p-1)(q-1)}$
- lub inaczej
  $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
- Liczby $d$ i $n$ są także względnie pierwsze

## 9.1 Algorytm RSA

- Wybieramy dwie duże liczby pierwsze: $\{p, q\}$
- Obliczamy ich iloczyn (łatwo): $n = pq$
- Wybieramy losowo liczbę $e < n$
  względnie pierwszą z liczbą $(p-1)(q-1)$
- Liczba $e$ będzie kluczem szyfrującym
- Znajdujemy liczbę $d$ taką, że
  $ed \equiv 1 \pmod{(p-1)(q-1)}$
- lub inaczej
  $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
- Liczby $d$ i $n$ są także względnie pierwsze

## 9.1 Algorytm RSA

- Wybieramy dwie duże liczby pierwsze: $\{p, q\}$
- Obliczamy ich iloczyn (łatwo): $n = pq$
- Wybieramy losowo liczbę $e < n$ względnie pierwszą z liczbą $(p-1)(q-1)$
- Liczba $e$ będzie kluczem szyfrującym
- Znajdujemy liczbę $d$ taką, że $ed \equiv 1 \pmod{(p-1)(q-1)}$
- lub inaczej $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
- Liczby $d$ i $n$ są także względnie pierwsze

## 9.1 Algorytm RSA

- Wybieramy dwie duże liczby pierwsze: $\{p, q\}$
- Obliczamy ich iloczyn (łatwo): $n = pq$
- Wybieramy losowo liczbę $e < n$ względnie pierwszą z liczbą $(p-1)(q-1)$
- Liczba $e$ będzie kluczem szyfrującym
- Znajdujemy liczbę $d$ taką, że $ed \equiv 1 \pmod{(p-1)(q-1)}$
- lub inaczej $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
- Liczby $d$ i $n$ są także względnie pierwsze

## 9.1 Algorytm RSA

- Wybieramy dwie duże liczby pierwsze: $\{p, q\}$
- Obliczamy ich iloczyn (łatwo): $n = pq$
- Wybieramy losowo liczbę $e < n$
  względnie pierwszą z liczbą $(p-1)(q-1)$
- Liczba $e$ będzie kluczem szyfrującym
- Znajdujemy liczbę $d$ taką, że
  $ed \equiv 1 \pmod{(p-1)(q-1)}$
- lub inaczej
  $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
- Liczby $d$ i $n$ są także względnie pierwsze

## 9.1 Algorytm RSA

- Wybieramy dwie duże liczby pierwsze: $\{p, q\}$
- Obliczamy ich iloczyn (łatwo): $n = pq$
- Wybieramy losowo liczbę $e < n$
  względnie pierwszą z liczbą $(p-1)(q-1)$
- Liczba $e$ będzie kluczem szyfrującym
- Znajdujemy liczbę $d$ taką, że
  $ed \equiv 1 \pmod{(p-1)(q-1)}$
- lub inaczej
  $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
- Liczby $d$ i $n$ są także względnie pierwsze

- Do obliczenia $d$ można użyć rozszerzonego algorytmu Euklidesa
- Liczba $d$ jest kluczem deszyfrującym
- Liczby $\{e, n\}$ stanowią klucz publiczny, który ujawniamy
- Liczby $\{d, n\}$ stanowią klucz prywatny, który powinien być ściśle chroniony (liczba $d$)

- Do obliczenia $d$ można użyć rozszerzonego algorytmu Euklidesa
- Liczba $d$ jest kluczem deszyfrującym
- Liczby $\{e, n\}$ stanowią klucz publiczny, który ujawniamy
- Liczby $\{d, n\}$ stanowią klucz prywatny, który powinien być ściśle chroniony (liczba $d$)

- Do obliczenia $d$ można użyć rozszerzonego algorytmu Euklidesa
- Liczba $d$ jest kluczem deszyfrującym
- Liczby $\{e, n\}$ stanowią klucz publiczny, który ujawniamy
- Liczby $\{d, n\}$ stanowią klucz prywatny, który powinien być ściśle chroniony (liczba $d$)

- Do obliczenia $d$ można użyć rozszerzonego algorytmu Euklidesa
- Liczba $d$ jest kluczem deszyfrującym
- Liczby $\{e, n\}$ stanowią klucz publiczny, który ujawniamy
- Liczby $\{d, n\}$ stanowią klucz prywatny, który powinien być ściśle chroniony (liczba $d$)

## 9.2 Szyfrowanie

Wiadomość dzielimy na bloki $m_i$ mniejsze niż $n$, które szyfrujemy używając formuły

$$c_i \equiv m_i^e \pmod{n}$$

## 9.2 Szyfrowanie

Wiadomość dzielimy na bloki $m_i$ mniejsze niż $n$, które szyfrujemy używając formuły

$$c_i \equiv m_i^e \pmod{n}$$

## 9.3 Deszyfrowanie

Tekst jawny z kryptogramu otrzymujemy obliczając

$$m_i \equiv c_i^d \pmod{n}$$

## 9.4 Uzasadnienie

Ponieważ $ed \equiv 1 \pmod{(p-1)(q-1)}$, to istnieje liczba całkowita $k$ taka, że $ed = 1 + k(p-1)(q-1)$. Z małego twierdzenia Fermata, dla $NWD(m,p) = 1$, mamy

$$m^{p-1} \equiv 1 \pmod{p}$$

Podnosząc obie strony tej kongruencji do potęgi $k(q-1)$ oraz mnożąc przez $m$ otrzymujemy

$$m^{1+k(p-1)(q-1)} \equiv m \pmod{p}$$

Kongruencja ta jest także prawdziwa dla $NWD(m,p) = p$, ponieważ wtedy obie strony przystają do $0 \pmod{p}$. Zatem, zawsze mamy

$$m^{ed} \equiv m \pmod{p}.$$

Podobnie,

$$m^{ed} \equiv m \pmod{q},$$

a ponieważ $p$ i $q$ są różnymi liczbami pierwszymi, to z chińskiego twierdzenia o resztach otrzymujemy

$$m^{ed} \equiv m \pmod{n}$$

# 9.5 Przykład (trywialny)

Znajdowanie klucza

# 9.5 Przykład (trywialny)

Znajdowanie klucza

$$p = 1123 \qquad q = 1237$$

## 9.5 Przykład (trywialny)

Znajdowanie klucza

$$p = 1123 \qquad q = 1237$$

$$n = pq = 1389151$$

# 9.5 Przykład (trywialny)

Znajdowanie klucza

$$p = 1123 \qquad q = 1237$$

$$n = pq = 1389151$$

$$\phi = (p-1)(q-1) = 1386792$$

# 9.5 Przykład (trywialny)

Znajdowanie klucza

$$p = 1123 \qquad q = 1237$$

$$n = pq = 1389151$$

$$\phi = (p-1)(q-1) = 1386792$$

$$e = 834781$$

# 9.5 Przykład (trywialny)

Znajdowanie klucza

$$p = 1123 \qquad q = 1237$$

$$n = pq = 1389151$$

$$\phi = (p-1)(q-1) = 1386792$$

$$e = 834781$$

$$d \equiv e^{-1} \pmod{\phi} = 1087477$$

# Szyfrowanie

# Szyfrowanie

$m = 983415$

# Szyfrowanie

$$m = 983415$$

$$c \equiv m^e \pmod{n}$$

# Szyfrowanie

$$m = 983415$$

$$c \equiv m^e \pmod{n}$$

$$e = 834781$$

# Szyfrowanie

$$m = 983415$$

$$c \equiv m^e \pmod{n}$$

$$e = 834781$$

$$n = 1389151$$

# Szyfrowanie

$$m = 983415$$

$$c \equiv m^e \pmod{n}$$

$$e = 834781$$

$$n = 1389151$$

$$983415^{834781} \pmod{1389151} = 190498$$

# Deszyfrowanie

# Deszyfrowanie

$$m \equiv c^d \pmod{n}$$

# Deszyfrowanie

$$m \equiv c^d \pmod{n}$$

$$c = 190498$$

# Deszyfrowanie

$$m \equiv c^d \pmod{n}$$

$$c = 190498$$

$$n = 1389151$$

# Deszyfrowanie

$$m \equiv c^d \pmod{n}$$

$$c = 190498$$

$$n = 1389151$$

$$d \equiv e^{-1} \pmod{\phi} = 1087477$$

# Deszyfrowanie

$$m \equiv c^d \pmod{n}$$

$$c = 190498$$

$$n = 1389151$$

$$d \equiv e^{-1} \pmod{\phi} = 1087477$$

$$190498^{1087477} \pmod{1389151} = 983415$$