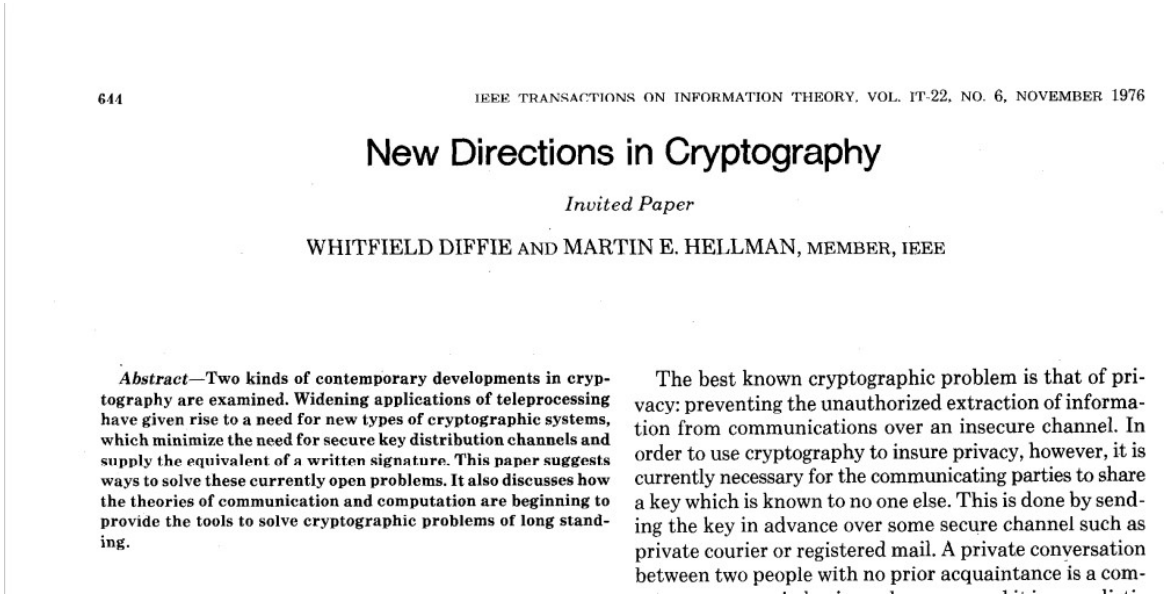
# Kryptografia asymetryczna

# Plan

1. Algorytm Diffie-Hellman’a
2. Algorytm RSA
3. Podpis cyfrowy
4. Certyfikat

# Rys historyczny

W 1976 roku amerykańscy kryptografowie Whitfield Diffie i Martin Hellman opublikowali pracę "Nowe kierunki w kryptografii", w której przedstawili koncepcję **wymiany kluczy publicznych**.



644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

*Invited Paper*

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

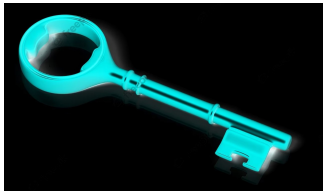
*Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a com-

# Klucz prywatny i publiczny

klucz prywatny jest w wyłącznym posiadaniu adresata (podpisującego)

klucz publiczny jest udostępniony każdemu, kto zechce zaszyfrować wiadomość (zweryfikować podpis)



# Potęgowanie i logarytmowanie

$\log_3 2\ 541\ 865\ 828\ 329 = ?$

3^26=2 541 865 828 329

# Modulo

25/7=3r4

25mod7=4

# GF(7) - ciało

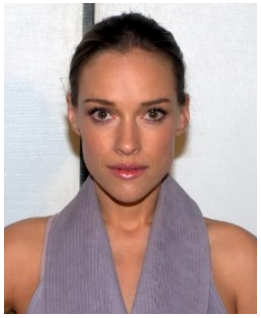
25mod7=4
26mod7=5
27mod7=6
28mod7=0
29mod7=1
30mod7=2
31mod7=3
32mod7=4 ...

# Uzgadnianie klucza

**Klucz: prywatny i publiczny**

3, 31

(3^26)mod31=18



26

18 >

< 22

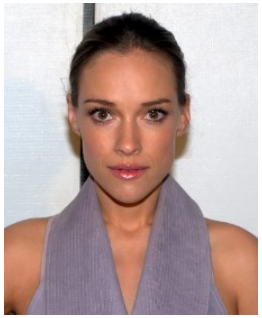
(3^17)mod31=22

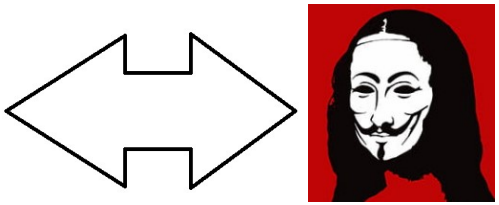
17

(22^26)mod31=14

(18^17)mod31=14

# Zagrożenia - Atak aktywny





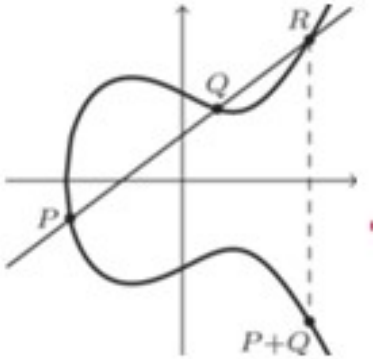
11

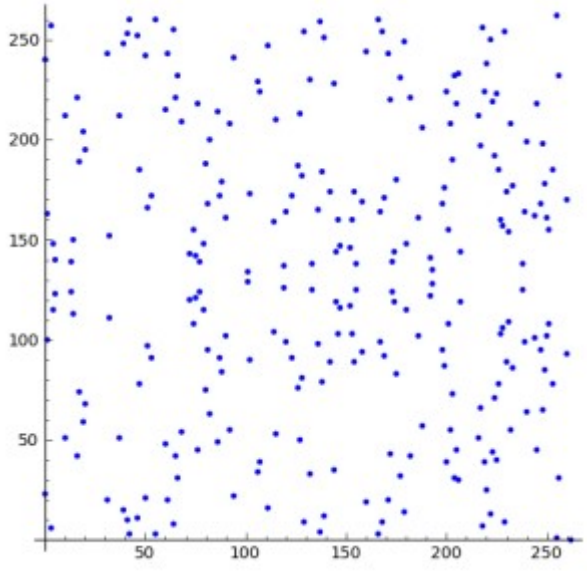


24

Man in the middle
(MITM)

# Krzywe eliptyczne



# Zad. 1 –uzgadnianie klucza- Algorytm RSA

openssl genpkey -algorithm RSA -out key.pem

openssl pkey -in key.pem -pubout -out pub_key.pub

(openssl asn1parse -in pub_key.pub)

openssl rand -hex 32 > klucz.hex

openssl pkeyutl -encrypt -in klucz.hex -pubin -inkey pub_key.pub -out ciph_key.hex

openssl pkeyutl -decrypt -in ciph_key.hex -inkey key.pem -out deciph_key.hex

# Szyfrowanie z wykorzystaniem algorytmów asymetrycznych

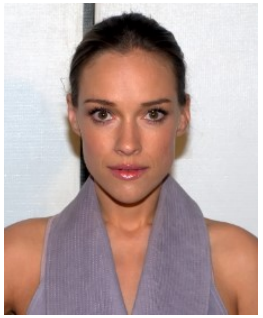
- **Klucz publiczny** używany jest do zaszyfrowania informacji, **klucz prywatny** do jej odczytu. Ponieważ klucz prywatny jest w wyłącznym posiadaniu adresata informacji, tylko on może ją odczytać. Natomiast klucz publiczny jest udostępniony każdemu, kto zechce zaszyfrować wiadomość.

- Kryptografia asymetryczna jest o wiele wolniejsza od tradycyjnej, nie szyfruje się wiadomości za pomocą kryptosystemów asymetrycznych. Zamiast tego szyfruje się jedynie klucz a następnie wykorzystuje się szyfrownanie symetryczne (strumieniowe lub blokowe)

# Podpisywanie z wykorzystaniem algorytmów asymetrycznych

- **klucz prywatny** używany jest do podpisania dokumentu elektronicznego. Ponieważ klucz prywatny jest w wyłącznym posiadaniu adresata informacji, tylko on może „obliczyć” konkretny podpis.
- **klucz publiczny** używany jest do weryfikacji podpisu. Klucz publiczny jest udostępniony każdemu, kto zechce zweryfikować podpis.

# Podpis cyfrowy (elektroniczny)



miejscowość ..... dnia . . .

**Sąd Okręgowy**
**I Wydział Cywilny**
**w Legnicy**

**Powódka/powód** : . . . (imię, nazwisko i dokładny adres z kodem pocztowym)

**Pozwany/pozwana**: . . . (imię, nazwisko i dokładny adres z kodem pocztowym)

**Pozew o rozwód**

**Wnoszę o:**

**I.** Rozwiązanie małżeństwa . . . (imię, nazwisko strony powodowej) . . . i . . . (imię, nazwisko strony pozwanej) . . . zawartego w dniu . . . (data zawarcia małżeństwa) . . . . . w USC . . . (miejscowość) . . . . . bez orzekania o winie/z winy powanego/z winy obu stron.[1] (niewłaściwe skreślić)

**II.** Powierzenie powódce/pozwanemu . . . (imię, nazwisko) . . . wykonywania władzy rodzicielskiej nad małoletnim synem/córką . . . (imię i nazwisko)..., ur. dnia . . . (data urodzenia dziecka) . . . w . . . (miejscowość urodzenia dziecka) . . .;

**III.** Nie orzekanie o kontaktach rodziców z małoletnim dzieckiem stron/ustalenie kontaktów rodziców z małoletnim dzieckiem stron po rozwodzie w następujący sposób : ..... (niewłaściwe skreślić);

**IV.** Zobowiązanie pozwanego/powódki do ponoszenia kosztów utrzymania syna/córki w kwocie . . . (kwota świadczeń alimentacyjnych) . . . złotych, płatnych do dnia ..... (np. 15-go) każdego kolejnego miesiąca.

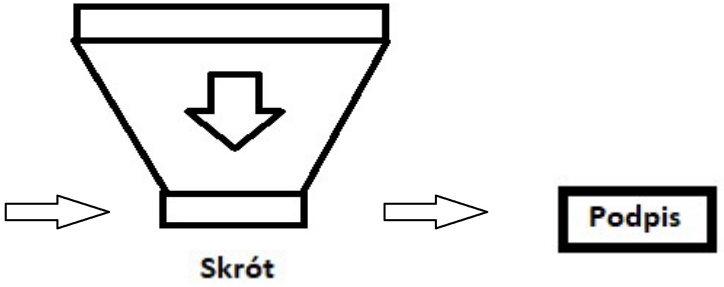
**V.** Zasądzenie od pozwanego na rzecz powódki kosztów procesu.

**Uzasadnienie**

. . . . . .

(własnoręczny podpis strony powodowej)

Załączniki:



# Podpis elektroniczny


miejscowość..... dnia . . .

Sąd Okręgowy
I Wydział Cywilny
w Legnicy

**Powódka/powód** : . . . (imię, nazwisko i dokładny adres z kodem pocztowym)

**Pozwany/pozwana**: . . . (imię, nazwisko i dokładny adres z kodem pocztowym)

**Pozew o rozwód**

**Wnoszę o:**

**I.** Rozwiązanie małżeństwa : . . (imię, nazwisko strony powodowej) . . . i . . . (imię, nazwisko strony pozwanej) . . . zawartego w dniu . . . (data zawarcia małżeństwa) . . . . . w USC . . . ; (miejscowość) . . . . - bez orzekania o winie/z winy pozwanego/z winy obu stron.' (niewłaściwe skreślić)

**II.** Powierzenie powódce/pozwanemu . . . (imię, nazwisko) . . . wykonywania władzy rodzicielskiej nad małoletnim synem/córką .....(imię i nazwisko).... ur. dnia . . . . (data urodzenia dziecka) . . w . . . (miejscowość urodzenia dziecka) . . . ;

**III.** Nie orzekanie o kontaktach rodziców z małoletnim dzieckiem stron/ustalenie kontaktów rodziców z małoletnim dzieckiem stron po rozwodzie w następujący sposób : ..... (niewłaściwe skreślić)

**IV**. Zobowiązanie pozwanego/powódki do ponoszenia kosztów utrzymania syna/córki w kwocie . . . (kwota świadczeń alimentacyjnych) . . . złotych, płatnych do dnia .....(np. 15-go) każdego kolejnego miesiąca.

**V**. Zasądzenie od pozwanego na rzecz powódki kosztów procesu.

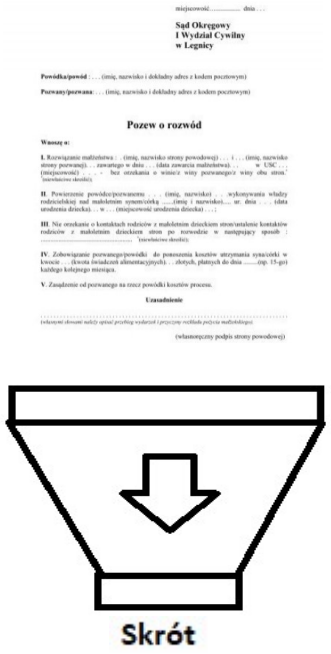
**Uzasadnienie**

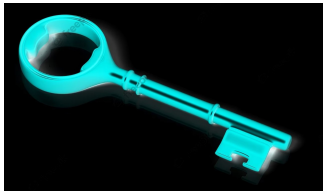
.....

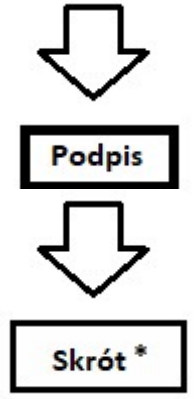
*(własnoręczny podpis strony powodowej)*

Załączniki:

Podpis






Skrót ? = Skrót *

# Podpis elektroniczny

Podpis cyfrowy zapewnia :
- Integralność - pozwala wykryć nieautoryzowane modyfikacje dokumentu po jego podpisaniu,
- autentyczność pochodzenia, która daje pewność co do autorstwa dokumentu,
- niezaprzeczalność, uniemożliwia wyparcie się autorstwa lub znajomości treści dokumentu.

# Podpis elektroniczny

Podpis cyfrowy ułatwia :

- Jest równoważny z podpisem odręcznym,

- Zastępuje dokumenty papierowe,

- Nie potrzebna fizyczna obecność w konkretnym miejscu przy podpisywaniu.

# Zad. 2. Podpis elektroniczny uproszczony

Podpis:

```
openssl genpkey -algorithm RSA -out private_key.pem

openssl pkey -in private_key.pem -pubout -out public_key.pem

openssl dgst -sha256 -sign private_key.pem -out umowa.sig umowa.txt
```

Weryfikacja:

```
openssl dgst -sha256 -verify public_key.pem -signature umowa.sig umowa.txt
```

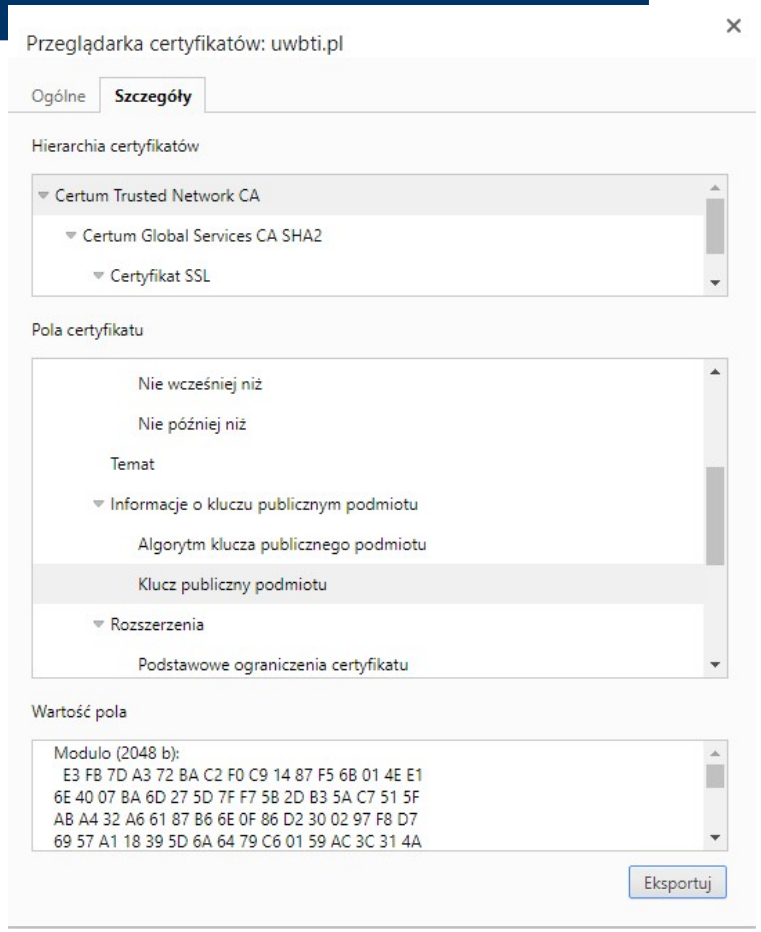
# Certyfikat (klucza publicznego)

Certyfikat to elektroniczny dokument, który zawiera informacje o tożsamości osoby lub organizacji oraz informacje o kluczu publicznym, który jest powiązany z tą tożsamością. Certyfikat zawiera następujące informacje:

- Informacje o tożsamości: certyfikat zawiera informacje o tożsamości osoby lub organizacji, która jest właścicielem klucza publicznego, w tym imię i nazwisko, adres, adres e-mail, numer telefonu i inne dane, które pozwalają zweryfikować tożsamość właściciela klucza.
- Informacje o kluczu publicznym: certyfikat zawiera informacje o kluczu publicznym, który jest powiązany z tożsamością właściciela, w tym algorytm szyfrowania, długość klucza, numer seryjny, datę wygaśnięcia certyfikatu i inne informacje.
- Informacje o wydającym certyfikat: certyfikat zawiera informacje o organizacji lub firmie, która wydała certyfikat, w tym nazwę, adres, numer telefonu i inne dane kontaktowe.
- Sygnatura cyfrowa: certyfikat zawiera sygnaturę cyfrową, która jest generowana na podstawie informacji zawartych w certyfikacie i klucza prywatnego wydającego certyfikat. Sygnatura cyfrowa zapewnia integralność certyfikatu i potwierdza, że certyfikat został wydany przez właściwą instytucję.

Certyfikaty są używane do uwierzytelniania serwerów internetowych, podpisów cyfrowych, szyfrowania poczty e-mail, VPN i wielu innych zastosowań, w których wymagane jest potwierdzenie tożsamości i poufność komunikacji.

# Certyfikat


Przeglądarka certyfikatów: uwbti.pl
Ogólne
Szczegóły
Hierarchia certyfikatów
Certum Trusted Network CA
Certum Global Services CA SHA2
Certyfikat SSL
Pola certyfikatu
Nie wcześniej niż
Nie później niż
Temat
Informacje o kluczu publicznym podmiotu
Algorytm klucza publicznego podmiotu
Klucz publiczny podmiotu
Rozszerzenia
Podstawowe ograniczenia certyfikatu
Wartość pola
Modulo (2048 b):
E3 FB 7D A3 72 BA C2 F0 C9 14 87 F5 6B 01 4E E1
6E 40 07 BA 6D 27 5D 7F F7 5B 2D B3 5A C7 51 5F
AB A4 32 A6 61 87 B6 6E 0F 86 D2 30 02 97 F8 D7
69 57 A1 18 39 5D 6A 64 79 C6 01 59 AC 3C 31 4A
Eksportuj

# Zad. 3. Podpis elektroniczny z certyfikatem

Podpis:

```
openssl genpkey -algorithm RSA -out key.pem

openssl req -new -key key.pem -x509 -out cert.pem

openssl dgst -sha256 -sign key.pem -out umowa.sig umowa.txt
```

Weryfikacja:

```
openssl x509 -pubkey -noout -in cert.pem > pubkey.pem

openssl dgst -sha256 -verify pubkey.pem -signature umowa.sig umowa.txt
```

# Podsumowanie

Diffie-Hellman – algorytm uzgadniania klucza seansowego,

RSA – algorytm asymetryczny, wykorzystywany w uzgadnianiu klucza seansowego, podpisie,

DSA – (ang. Digital Signature Algorithm) algorytm podpisu elektronicznego.

# Kryptografia asymetryczna

THE END