

Bezpieczeństwo komputerowe - lista

4

Bartosz Biegalski, 272347

1.1 Program do obliczenia klucza prywatnego

Sama operacja łamania kodu opiera się na pętli, w której ze znajomości parametrów (n , e , d) staramy się wyznaczyć jedną z liczb pierwszych t , że $p \cdot q = n$.

```
a = 2
while (True):
    k = t
    while k < kphi:
        x = pow(a, k, n)
        if x != 1 and x != (n - 1) and x ** 2 % n == 1:
            r = sympy.gcd(x - 1, n)
            return n // r
        k *= 2
    a += 2
```

1.2 Przykładowe dane wejściowe i wyniki

Bezpieczne długości kluczy to takie mające długość od 2048, czasem 4096. Niestety, samo szukanie tak dużych liczb pierwszych może zajmować ogromną ilość czasu, a co dopiero operacje na nich. Mój program działa poprawnie na relatywnie “małych” liczbach pierwszych.

```
bartek@bartek-Lenovo-Legion-5-15IMH05: ~/Documents/Study/sem4/bb/11stade/ci/Python$ python3 z1.py 33573971 33573977
skA: (1127211730152667, 656724134796567)
pkA: (1127211730152667, 878589412000343)
skB: (1127211730152667, 598588697569203)
pkB: (1127211730152667, 591026137539147)
Odkryty klucz prywatny dla osoby A: (1127211730152667, 656724134796567)
```

```
bartek@bartek-Lenovo-Legion-5-15IMH05: ~/Documents/Study/sem4/bb/11stade/ci/Python$ python3 z1.py 252097800667 252097800623
skA: (63553301090046162415541, 35984606011695119188873)
pkA: (63553301090046162415541, 9121594555169560731205)
skB: (63553301090046162415541, 16366660867131703391149)
pkB: (63553301090046162415541, 50391358961226615379261)
Odkryty klucz prywatny dla osoby A: (63553301090046162415541, 35984606011695119188873)
```

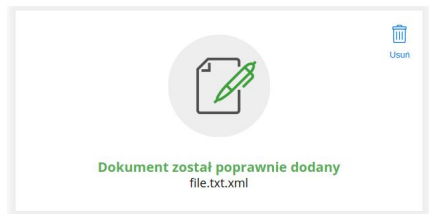
2.1 Profil zaufany, podpis zaufany

Z rządowej strony o profilu zaufanym dowiedziałem się, że każdy obywatel Polski (także cudzoziemiec z numerem PESEL) posiadający ważny numer PESEL. Profil ów służy do szeroko pojętego załatwiania spraw urzędowych online, a do weryfikacji wykorzystuje dane osobowe i 2FA, najczęściej przez kod wysłany SMS.

Podpis zaufany jest sposobem na weryfikację osobistą, pozwalającą podejmować czynności prawne bez potrzeby pojawiania się w urzędzie. Potwierdzenie podpisu dokonuje się również poprzez podanie kodu otrzymanego w SMS.

2.2 Podpisanie pliku txt i pdf, następnie weryfikacja poprzez portal gov

Podpisane dokumenty można także zweryfikować na stronie podpisu zaufanego. Formaty XAdES i PAdES to Advanced Electronic Signatures, z czego XAdES zapisuje plik z podpisem do pliku z rozszerzeniem .xml. Taki podpis jest zagnieżdżony w plik podpisywany, możliwe jest też otrzymanie osobnego pliku nie połączonego z podpisywanym. Format PAdES odnosi się do plików PDF, a podpis zaufany pozwala na umieszczenie znaku wodnego, który symbolizuje podpis.



Właściciel podpisu: **BARTOSZ BIEGALSKI**
Data i godzina podpisu: **2024-05-13 21:12:39 CEST**
Status podpisu: **✓ Ważny**
Rodzaj podpisu: **Podpis zaufany**



watermark umieszczony na pliku pdf

2.3 Weryfikacja podpisów poprzez serwis Madkom



Madkom SA zajmuje się m.in. weryfikacją podpisów zaufanych, chociaż nie figuruje w rejestrze dostawców usług zaufania

(<https://www.nccert.pl/uslugi.htm>). To znaczy, że ich ekspertyza odnośnie podpisów wydaje się być bardzo profesjonalna, ale jest póki co wiążąca.

Madkom SA zwraca następujące informacje: podpis został wystawiony na podpisującego (na mnie) w imieniu ministra cyfryzacji. Nie znajduje się na liście CRL, czyli w spisie unieważnionych certyfikatów dostawców usług zaufania.

| | |
|---|--|
|  | lista3podpisana.pdf md5: b3e5234a9944d3769da06894a57d8e40 |
|  | Integralność: Zachowana - podpisane dane nie zostały zmodyfikowane od czasu ich elektronicznego uwierzytelnienia |
|  | Podpisujący: BARTOSZ BIEGALSKI |
|  | Rodzaj uwierzytelnienia: Podpis zaufany (Minister do spraw informatyzacji - pieczęć podpisu zaufanego) |
|  | Deklarowany czas złożenia podpisu: 2024-05-13 19:21:27+00:00 ⓘ |

Pełna ścieżka certyfikacji

- ✓ Narodowe Centrum Certyfikacji  +
-  ✓ Centrum Kwalifikowane EuroCert  +
-  ✓ Minister do spraw informatyzacji - pieczęć podpisu zaufanego  +

Certyfikat został zweryfikowany za pomocą:

✓ Certyfikat nie znajduje się na liście CRL ⓘ

2.4 Zmiana pliku podpisanego usługą podpisu zaufanego

Serwis Weryfikacja podpisu firmy Madkom nie wykrywa podpisu w zmienionym pliku pdf oznaczonym podpisem PAdES.



Zmiana pliku podpisanego XAdES-em także uniemożliwia przeczytanie go i w efekcie weryfikację przez powyższy serwis. Podobny wynik zwraca rządowa strona.



Właściciel podpisu:

Data i godzina podpisu:

Status podpisu:  **Nieważny**

Rodzaj podpisu: **Podpis kwalifikowany**

| | |
|---|---|
|  | Uwierzytelnienie e-dokumentu nie jest możliwe |
|  | Weryfikator nie wykrył wśród przestanych plików żadnego pliku z podpisem. |

| | |
|---|--|
|  | file.txt.xml md5: dfae16de5411d09b3ab9d30b668be33b |
|  | Nieobstługiwana struktura podpisu |

2.5 Weryfikacja pdf podpisanego przez Panią Lauks, rodzaje profili

PDF przekazany od Pani Lauks został pozytywnie zweryfikowany przez serwis weryfikacjapodpisu.pl. Jednak wystawca podpisu został zakwalifikowany jako niezaufany, co oznacza że nie figuruje na liście zaufanych dostawców, która znajduje się tutaj:

<https://www.nccert.pl/uslugi.htm>.

Podpis osobisty jest najbardziej podstawową wersją weryfikacji danych osobowych przez Internet i dostęp do infrastruktury administracji publicznej w Polsce. Podpis zaufany pozwala na dodatkowe aktywności, m.in na wspomniane podpisy zaufane. Podpis kwalifikowany umożliwia załatwianie spraw urzędowych, ale też na przykład zawieranie umów na odległość, branie udział w aukcjach przetargowych. Po podpis kwalifikowany trzeba specjalnie wystąpić i jest to usługa płatna.