Security: RSA

Liczby używane w szyfrowaniu RSA

W szyfrowaniu RSA ważne są liczby pierwsze, ponieważ algorytm opiera się na faktoryzacji dużych liczb. W celu dobrania liczb do algorytmu RSA wybiera się dwie liczby pierwsze p i q.

Przykładowe liczby:

- 57: nie jest liczbą pierwszą (57 = 3 × 19).
- 67: jest liczbą pierwszą.
- 77: nie jest liczbą pierwszą (77 = 7 × 11).
- 97: jest liczbą pierwszą.

Funkcja Eulera

Funkcja Eulera ϕ to funkcja matematyczna, która dla każdej liczby całkowitej n zwraca liczbę liczb całkowitych dodatnich mniejszych od n, które są względnie pierwsze z n (tj. mają największy wspólny dzielnik równy 1). Funkcja ta jest użyteczna w teorii liczb, szczególnie w kontekście kryptografii, zwłaszcza w algorytmie RSA.

Wzór

Dla liczby pierwszej p:

$\phi(p)=p−1$

Dla liczby n będącej iloczynem dwóch różnych liczb pierwszych p i q:

$\phi(n)=(p−1)(q−1)$

Obliczenia dla 53 i 71

$$ p = 51 \\ q = 71 \\ \phi = (p-1)(q-1) \\ \phi = (53-1)(71-1) = 52 * 40 = 3640 \\ $$

Szyfrowanie i deszyfrowanie w systemie RSA

RSA to jedna z najpopularniejszych metod kryptografii asymetrycznej, która wykorzystuje parę kluczy: publiczny do szyfrowania i prywatny do deszyfrowania.

Klucz RSA

Aby wygenerować klucz RSA, wykonujemy następujące kroki:

Wybór dwóch dużych liczb pierwszych:

- Niech p i q będą dwoma liczbami pierwszymi. Na przykład:
  - $p=61$
  - $q=53$

Obliczenie n:

- $n=p*q$
- $n=61*53=3233$

Obliczenie funkcji Eulera $\phi(n)$:

- $\phi(n)=(p−1)(q−1)$
- $\phi(n)=(61−1)(53−1)=60*52=3120$

Wybór wykładnika publicznego e:

- Wybieramy e takie, aby było względnie pierwsze z $\phi(n) (1 < e < \phi(n))$. Najczęściej wybieranym e jest 65537, ale w tym przykładzie weźmiemy $e=17$.

Można sprawdzić tutaj: https://www.calculatorsoup.com/calculators/math/gcf.php

Obliczenie wykładnika prywatnego d:

- Musimy znaleźć d tak, aby spełniał równanie: $d*e≡1 \mod \phi(n)$
- Używając algorytmu rozszerzonego Euklidesa, otrzymujemy d=2753.

Klucze

- Klucz publiczny: $(e,n)=(17,3233)$
- Klucz prywatny: $(d,n)=(2753,3233)$

Szyfrowanie

Aby zaszyfrować wiadomość m, używamy klucza publicznego (e,n):

* Obliczenie szyfrogramu $c: c=m^e \mod n$

Na przykład, jeśli $m = 123$:

$c = 12317 \mod 3233$

Obliczenia prowadzą do $c=855$ (po pełnych wyliczeniach).

Deszyfrowanie

Aby odszyfrować szyfrogram c, używamy klucza prywatnego (d,n):

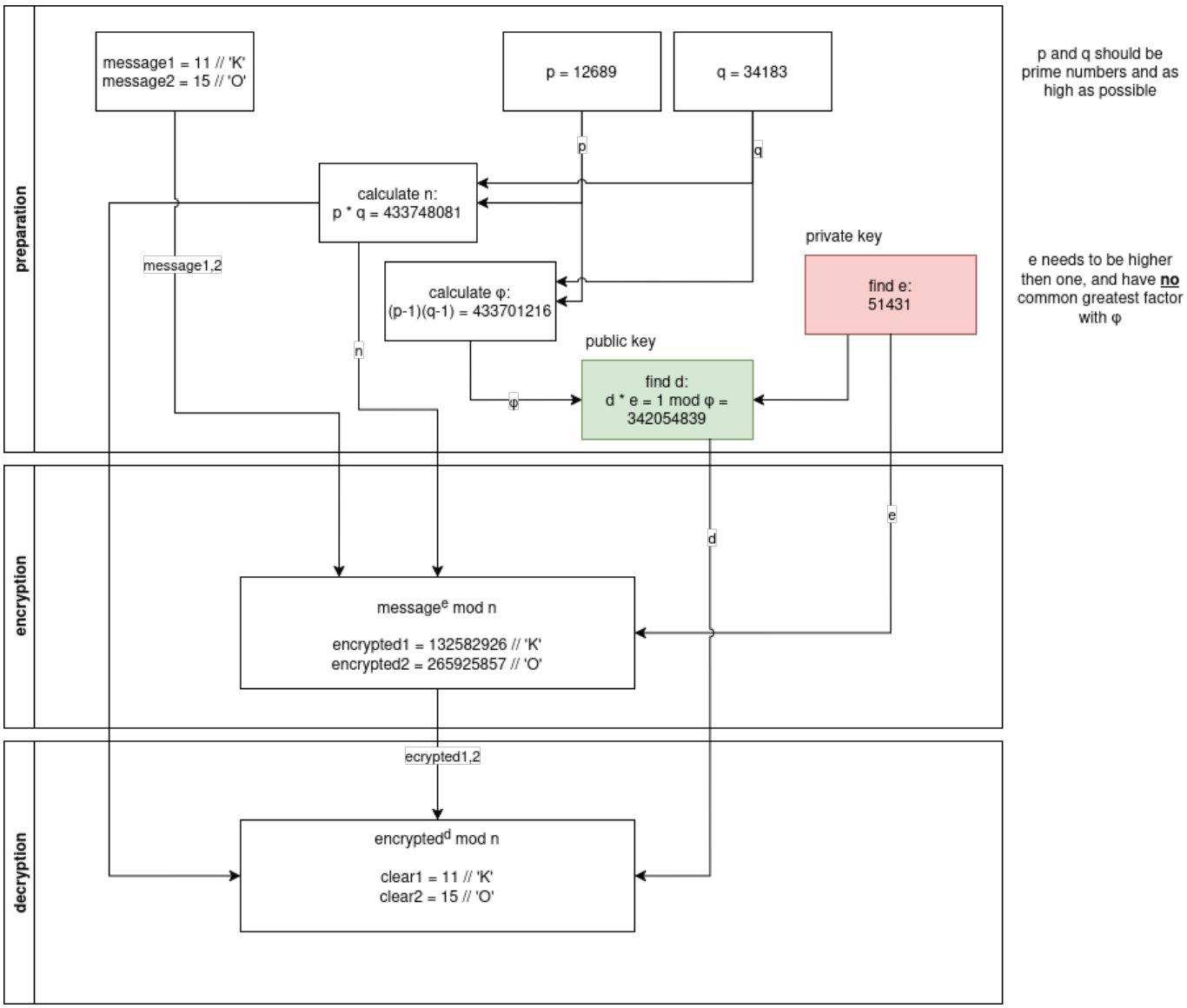
- Obliczenie odszyfrowanej wiadomości $m: m=c^d \mod n$

Dla $c = 855$:

$m = 8552753 \mod 3233$

Obliczenia prowadzą do $m=123$.

Flowchart



Program

https://github.com/DavidoTek/rsa-calc-edu

https://wiki.ostrowski.net.pl/php_mysql/rsa/