Security: RSA

Numbers used in RSA encryption

In RSA encryption, prime numbers are important because the algorithm is based on factorisation of large numbers. In order to select numbers for the RSA algorithm, two prime numbers p and q are chosen.

Example numbers:

- 57: is not a prime number (57 = 3 × 19).
- 67: is a prime number.
- 77: is not a prime number (77 = 7 × 11).
- 97: is a prime number.

Euler function

The Euler function $$ is a mathematical function that, for any integer n, returns the number of positive integers less than n that are relatively prime of n (i.e. have a greatest common divisor equal to 1). This function is useful in number theory, particularly in the context of cryptography, especially in the RSA algorithm. ==== Formula ==== For the number n being the product of two different prime numbers p and q: $phi(n)=(p-1)(q-1)$

Calculations for 53 and 71

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

RSA encryption and decryption

RSA is one of the most popular methods of asymmetric cryptography, which uses a pair of keys: public for encryption and private for decryption.

RSA key

To generate an RSA key, we follow the following steps:

Selection of two large prime numbers:

- Let p and q be two prime numbers. For example:
  - $p=61$
  - $q=53$

Calculation of n:

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

Calculation of Euler's function $phi(n)$:

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

Selection of the public exponent e:

- We choose e such that it is relatively prime with $\phi(n) (1 < e < \phi(n))$. 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):

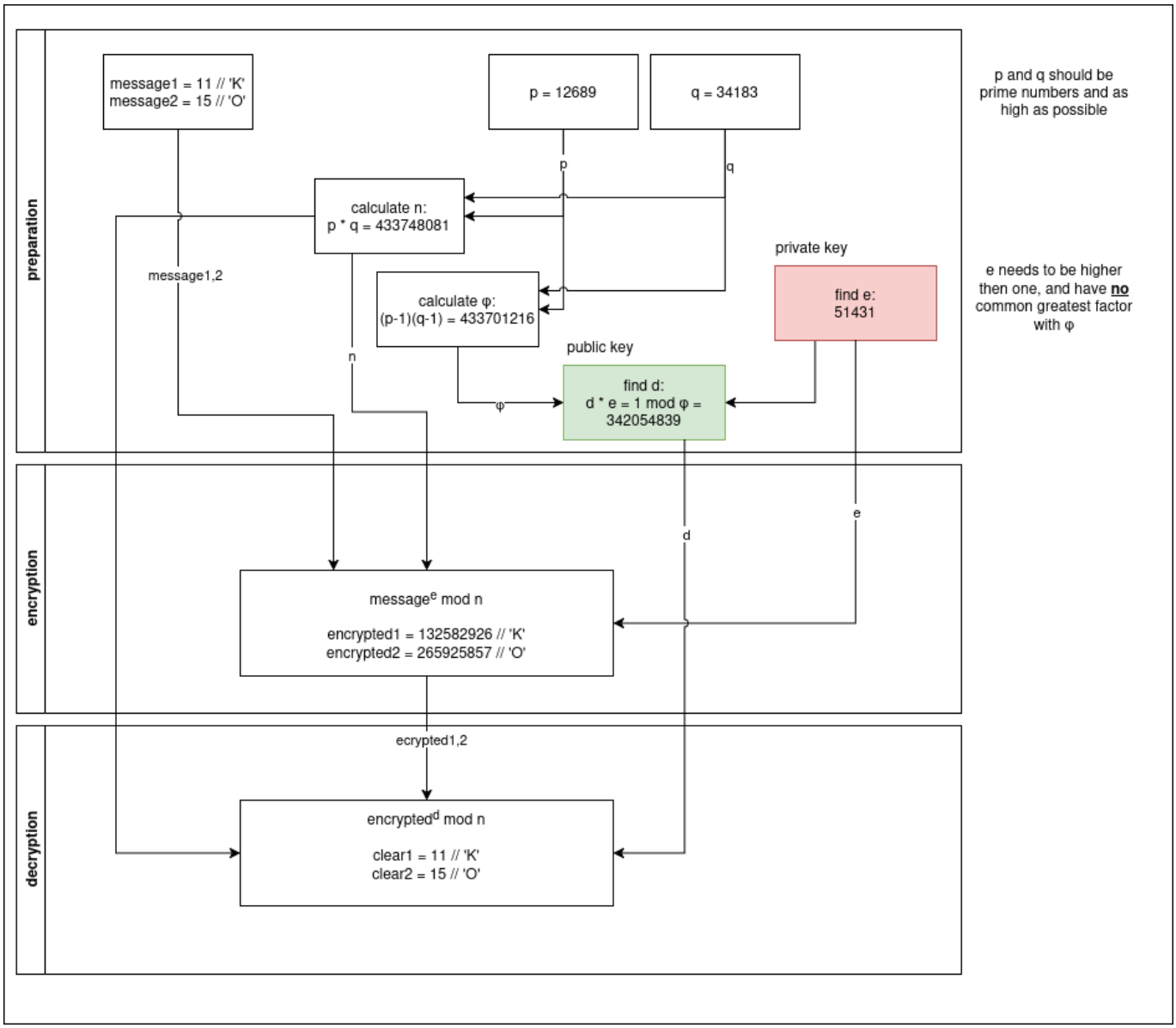
- Obliczenie odszyfrowanej wiadomości $m: m=c^d \mod n$

Dla $c = 855$:

$m = 8552753 \mod 3233$

Obliczenia prowadzą do $m=123$.

Flowchart



Programme

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

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