3'rd tutorial: RSA - encryption

Př: Design an RSA-protokol for encrypting messages $a < 2^8 = 256$.

—

We want modulus $n = pq > 256$, which holds for $p = 13$, $q = 23$ primes.

Now $n = 13 \cdot 23 = 299$

$\varphi(n) = 12 \cdot 22 = 264$

We choose $e = 5$ relatively prime to $\varphi(n)$.

We count $d = 5^{-1}$ in $\mathbb{Z}_{264}$ Eukleid. algor (or we could guess d, since $5 \cdot 53 = 265 = 1$ in $\mathbb{Z}_{264}$

$d = 53$.

Public key: $(n, e) = (299, 5)$.

Private key: $(n, d) = (299, 53)$.

Př: Alice's public key is $(n, e) = (517, 11)$. Which of the following pairs is Alice's private key ?

$(571, 67)$; $(517, 301)$; $(517, 251)$

—

$(571, 67)$ - NO, different modulus n

$(517, 301)$ - either we try for some $a < 517$, if $(a^{11})^{301} = a$ in $\mathbb{Z}_{517}$,

or we can use brute force to faktorize n

$n = 517$, $\sqrt{n} \doteq 22$ - we divide by primes $3, 5, \dots, 19$

finally $n = 11 \cdot 47$

$\varphi(n) = 10 \cdot 46 = 460$

we check if $ed = 1$ in $\mathbb{Z}_{\varphi(n)}$

$11 \cdot 301 = 3311 = 91$ in $\mathbb{Z}_{460}$

$\to 301 \neq d$

$(517, 251)$ we shoud check, if $ed = 1$ in $\mathbb{Z}_{\varphi(n)}$:

$11 \cdot 251 = 2761 = 1$ in $\mathbb{Z}_{460}$

$\to d = 251$

this is Alice's private key.

Př: Alice has a public key $(n_A, e_A) = (517, 11)$, a private key $(n_A, d_A) = (517, 251)$,

Bob has a public key $(n_B, e_B) = (533, 17)$, e private key $(n_B, d_B) = (533, 113)$.

Bob wants to send Alice a message $a = 10$. How will he encrypt it ?

—

Bob uses Alice's public key and counts $b = a^{e_A}$ in $\mathbb{Z}_{n_A}$.

$b = 10^{11}$ in $\mathbb{Z}_{517}$

He does it by repeated squaring: $11 = 8+2+1 = (1\,0\,1\,1)_2$ $\;\times S\, S \times S \times$

$$\mathbb{Z}_{517}: \quad 1 \xrightarrow{\times} 10 \xrightarrow{S} 100 \xrightarrow{S} 10\,000 = 177 \xrightarrow{\times} 1770 = 219 \xrightarrow{S}$$
$$\xrightarrow{S} 47\,961 = 397 \xrightarrow{\times} 3\,970 = 351$$

The encrypted message $\underline{b = 351}$ will Bob send to Alice.

Př: Alice has a public key $(n,e) = (551, 11)$. Bob sent to Alice a message $b = 169$. Eve captured the message and decrypted it by brute force attack.

Brute force attack: $\sqrt{n} \doteq 23$, we divide by primes ≤ 23, we get $n = 19 \cdot 29$.

$\varphi(n) = 18 \cdot 28 = 504$

$d = 11^{-1}$ in $\mathbb{Z}_{504}$

we solve $11 d + 504 k = 1$ in $\mathbb{Z}$ Extended Eukleid. alg.

$$\left(\begin{array}{cc|c} 1 & 0 & 11 \\ 0 & 1 & 504 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & 11 \\ -50 & 1 & -46 \end{array}\right)_{R_2 - 50R_1} \sim \left(\begin{array}{cc|c} -229 & 5 & 1 \\ -46 & 1 & -2 \end{array}\right) \begin{array}{l} R_1 + 5R_2 \\ R_2 + 4R_1 = \check{R}_2 \end{array}$$

so $-229 \cdot 11 + 5 \cdot 504 = 1$

Alice's private key is $d = 11^{-1} = -229 = 275$ in $\mathbb{Z}_{504}$.

Decryption could be done residually, since we know $p = 19$, $q = 29$.

in $\mathbb{Z}_{19}$ $\quad a = b^d = 169^{275} = (-2)^5 = -32 = 6$

E.-F. exponent modulo $\varphi(19) = 18$.

in $\mathbb{Z}_{29}$ $\quad a = b^d = 169^{275} = (-5)^{23} = \quad = 25$

E.-F. in exp. mod $\varphi(29) = 28$

repeated squaring $23 = 16 + 4 + 2 + 1 = (1\,0\,1\,1\,1)$ $\;\times S\, S \times S \times S \times$

$$1 \xrightarrow{\times} (-5) \xrightarrow{S} 25 = (-4) \xrightarrow{S} 16 \xrightarrow{\times} -80 = 7 \xrightarrow{S} 49 = -9 \xrightarrow{\times} 45 = -13 \xrightarrow{S}$$
$$\xrightarrow{S} 169 = (-5) \xrightarrow{\times} 25$$

$\mathbb{Z}_{19 \cdot 29} = \mathbb{Z}_{551}$ $\quad a = b^d = 6 \cdot g_{19} + 25 \cdot g_{29}$

where $g_{19} = 29t$, $g_{29} = 19r$ so that $29t + 19r = 1$

$$\left(\begin{array}{cc|c} 1 & 0 & 19 \\ 0 & 1 & 29 \end{array}\right) \sim \left(\begin{array}{cc|c} 3 & -2 & -1 \\ -1 & 1 & 10 \end{array}\right) \begin{array}{l} R_1 - 2\check{R}_2 \\ R_2 - R_1 = \check{R}_2 \end{array}$$

$-R_1$: $\underbrace{-3 \cdot 19}_{g_{29} = -57} + \underbrace{2 \cdot 29}_{g_{19} = 58} = 1$

The decrypted message is $a = 6 \cdot 58 + 25 \cdot (-57) = -1077 = 25$.
(in $\mathbb{Z}_n = \mathbb{Z}_{551}$)

Knowledge of $\varphi(n)$ or of the private key allows to find the faktorization of n.

Př: For $n = 6683$ (modulus of RSA-protokol) we know $\varphi(n) = 6480$.
Faktorize n.

It holds: $n = pq = 6683$, $\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1 = 6480$

so $p+q = n - \varphi(n) + 1 = 6683 - 6480 + 1 = 204$

p, q are roots of polyn. $(x-p)(x-q) = x^2 - (p+q)x + pq$

we solve : $x^2 - 204x + 6683 = 0$

$$D = (-204)^2 - 4 \cdot 6683 = 14884 \ , \ \sqrt{D} = 122$$

$$p, q = \frac{204 \pm 122}{2} = 102 \pm 61 = \begin{cases} 41 \\ 163 \end{cases}$$

Faktorization $n = 6683 = 41 \cdot 163$.

Př: Bob's RSA-key is $(n,e) = (533, 17)$, $(n,d) = (533, 113)$.
Faktorize n from knowledge of e and d.

It holds: $ed = 1$ in $\mathbb{Z}_{\varphi(n)}$, i.e. $ed - 1 = k \cdot \varphi(n) = k(p-1)(q-1)$ - even, divisible by 4

E.-F th. says : for any $a \in \mathbb{Z}_n^*$ $a^{ed-1} = \left(a^{\varphi(n)}\right)^k = 1$ in $\mathbb{Z}_n$

We want to find nontriv. $\sqrt{1}$, i.e. $b \neq \pm 1$, $b^2 = 1$ in $\mathbb{Z}_n$

since than $\underbrace{(b-1)}_{\neq 0}\underbrace{(b+1)}_{\neq 0} = b^2 - 1 = 0$ in $\mathbb{Z}_n$

$b-1, b+1$ are zero-divisors in $\mathbb{Z}_n$, thus $\gcd(b-1, n) = p$
$\gcd(b+1, n) = q$.

$ed - 1 = 1920 = 2^7 \cdot 15$

We choose $a = 2$ and we power in $\mathbb{Z}_n = \mathbb{Z}_{533}$

$$2 \xrightarrow{(\cdot)^{15}} 2^{15} = 255 \xrightarrow{S} 532 = (-1) \xrightarrow{S} 1 \qquad \text{KO , we found } \sqrt{1} = -1.$$

We choose $a = 3$

$$3 \xrightarrow{(\cdot)^{15}} 3^{15} = 14 \xrightarrow{S} 196 \xrightarrow{S} 40 \xrightarrow{S} 1 \qquad \text{OK , we have } b = \sqrt{1} = 40$$

We count $p = \gcd(b-1, n) = \gcd(39, 533)$ Eukleid. alg. .

$p = 13$; $q = \frac{n}{p} = 41 = \gcd(b+1, n)$.

$533 = 13 \cdot 39 + 26$
$39 = 1 \cdot 26 + 13$
$26 = 2 \cdot 13 + 0$.

Faktorization $n = 533 = 13 \cdot 41$.

HW: 1) Alice has a public key for RSA $(n,e) = (1121, 95)$. You have caught an encrypted message for Alice $b = 701$. Decrypt it by brute force attack.
[Solution: $d = 11$, message $a = 555$.]

2) Faktorize $n = 2231$ by knowledge of $\varphi(n) = 2112$. [$n = 23 \cdot 97$]