UNIVERSITY OF TWENTE.

THS Cryptography workshop

RSA

Federico Mazzone (f.mazzone@utwente.nl)

RSA

- Public modulus $n = pq$
- Public exponent e
- Private exponent d such that $ed = 1 \pmod{\phi(n)}$ where $\phi(n) = (p-1)(q-1)$
- Encryption $c = m^e \pmod{n}$
- Decryption $m = c^d \pmod{n}$

Conditions

Necessary

- p, q primes
- $\gcd\big(e, \phi(n)\big) = 1$

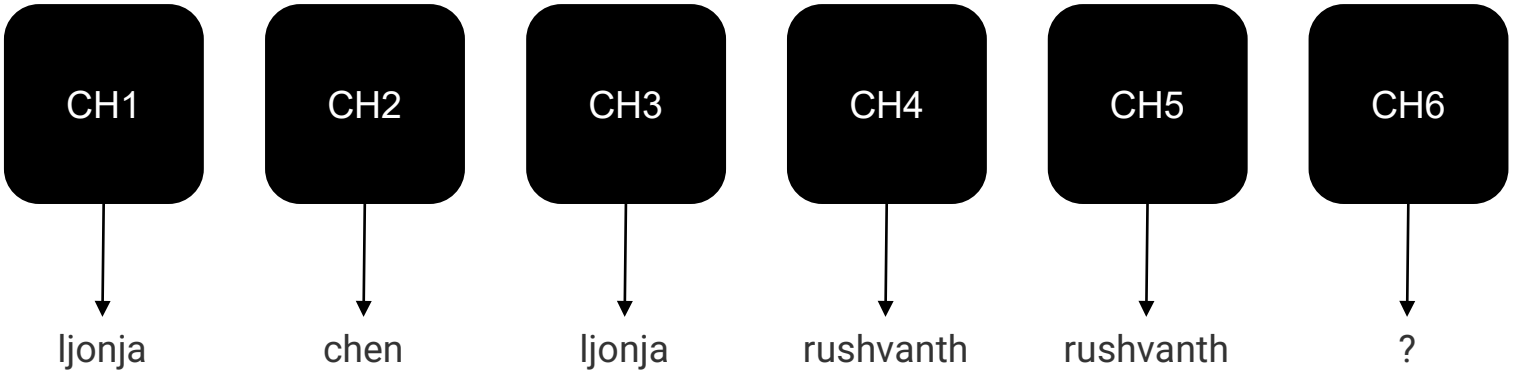
For security reasons

- p, q same magnitude
- p, q distant enough
- $m \geq n^{1/e}$
- p, q safe / strong primes

Let’s play – Game rules

- There are 6 challenges on the THS website (https://ths.eemcs.utwente.nl/) named “RSA challenge X”.
- The challenges have been sorted by difficulty.
- The first who submit the flag of a challenge and is able to explain his/her solution will get the corresponding prize.
- You can team up if you wish, but then you will have to handle the prize splitting ;)
- Maximum 2 prizes per team.
- If too much time pass without any submission, hints will be given on the easiest unsolved challenge.

Competition results



Ch4 – Fermat

Target = write n as the difference of 2 squares

$$n = a^2 - b^2 = (a + b)(a - b)$$

Start with $a = \lceil \sqrt{n} \rceil$. Loop:

1. If $n - a^2$ is a square, return $a + \sqrt{n - a^2}$.
2. Increment a by 1.

Ch5 – Common modulus attack

Two public keys $(n, e_1), (n, e_2)$ with common modulus and coprime exponents.
A single message m is encrypted with the two keys:

$$c_1 = m^{e_1} \pmod{n}$$
$$c_2 = m^{e_2} \pmod{n}$$

Attack idea:

$$\exists s_1, s_2 : e_1 s_1 + e_2 s_2 = \gcd(e_1, e_2)$$
$$m = m^1 = m^{\gcd(e_1, e_2)} = m^{e_1 s_1 + e_2 s_2} = m^{e_1 s_1} m^{e_2 s_2} = (m^{e_1})^{s_1} (m^{e_2})^{s_2} = {c_1}^{s_1} {c_2}^{s_2}$$

Ch6 – Linear relations

$$m_2 = m_1 + 2$$

$$c_2 = m_2^3 = (m_1 + 2)^3 = m_1^3 + 6m_1^2 + 12m_1 + 8$$

$$c_2 - c_1 = 6m_1^2 + 12m_1 + 8$$

Ch7 – Pollard p-1

$$a^{p-1} = 1 \pmod{p} \quad \Longrightarrow \quad p \mid a^{k(p-1)} - 1 \quad \Longrightarrow \quad p \mid \gcd\left(a^{k(p-1)} - 1, n\right)$$

If $p-1$ is B-smooth, you can test last relation for random a^Q, where Q is the product of all powers $\leq n$ of primes $\leq B$.

Ch8 – Small encryption exponent (CRT)

Given $n_1, \dots, n_k$ coprime and given $a_1, \dots, a_k$ with $a_i \in \mathbb{Z}_{n_i}$, then

$$\exists!\, x \in \mathbb{Z}_{n_1 \cdots n_k} \; : \; \begin{cases} x = a_1 \pmod{n_1} \\ \vdots \\ x = a_k \pmod{n_k} \end{cases}$$

Reference for further crypto knowledge

- Handbook of Applied Cryptography
  https://cacr.uwaterloo.ca/hac/

Reference for further crypto challenges

- CryptoHack
  https://cryptohack.org/

UNIVERSITY OF TWENTE.