

# Rabin cryptosystem

Martin Stanek

Department of Computer Science  
Comenius University  
`stanek@dcs.fmph.uniba.sk`

Cryptology 1 (2020/21)

# Content

Quadratic residues

Rabin cryptosystem

# Quadratic residues

- ▶ an integer  $a \in \mathbb{Z}_n^*$  is called a *quadratic residue* modulo  $n$  if there exists an integer  $b$  such that  $b^2 \equiv a \pmod{n}$
- ▶ otherwise  $a$  is called a quadratic nonresidue modulo  $n$
- ▶  $QR_n$  – the set of all quadratic residues modulo  $n$
- ▶  $QNR_n$  – the set of all quadratic nonresidues modulo  $n$
- ▶ trivially  $QR_n \cup QNR_n = \mathbb{Z}_n^*$

# Quadratic residues modulo prime

example for  $p = 11$ :

$x$	1	2	3	4	5	6	7	8	9	10
$x^2 \bmod 11$	1	4	9	5	3	3	5	9	4	1

## Lemma 1

Let  $p > 2$  be a prime. Then  $|QR_p| = |QNR_p|$ .

## Proof.

Let  $x^2 \equiv y^2 \pmod{p}$  for any  $x, y \in \mathbb{Z}_p^*$ . Then

$$p \mid (x^2 - y^2) \quad \Rightarrow \quad p \mid (x - y)(x + y).$$

We have  $x = y$  or  $x = p - y$ , i.e. each quadratic residue has exactly two square roots. Therefore  $|QR_p| = |\mathbb{Z}_p^*|/2 = (p - 1)/2 \Rightarrow |QNR_p| = (p - 1)/2$   $\square$

# Computing square roots modulo prime

- ▶ solve equation  $x^2 \equiv a \pmod{p}$
- ▶ solution exists iff  $a \in \text{QR}_p$
- ▶ if  $x$  is the solution then  $-x = p - x$  is the solution as well:  
 $(p - x)^2 \equiv p^2 - 2px + x^2 \equiv x^2 \equiv a \pmod{p}$
- ▶ easy to solve for  $p \equiv 3 \pmod{4}$ ; the solution is  $x = a^{(p+1)/4} \pmod{p}$ :

$$\begin{aligned}x^2 &\equiv a^{(p+1)/2} \equiv a \cdot a^{(p-1)/2} \pmod{p} \\&\equiv a \cdot b^{p-1} \pmod{p} && \text{(assuming } a \in \text{QR}_p, \text{ i.e. } \exists b: b^2 \equiv a) \\&\equiv a \pmod{p} && \text{(FLT)}\end{aligned}$$

- ▶ probabilistic polynomial time (PPT) algorithm exists for  $p \equiv 1 \pmod{4}$

# Euler's criterion: testing $a \in \text{QR}_p$ ?

## Lemma 2 (Euler's criterion)

Let  $p > 2$  be a prime and  $a \in \mathbb{Z}_p^*$ . Then  $a \in \text{QR}_p \Leftrightarrow a^{(p-1)/2} \equiv 1 \pmod{p}$ .

Proof.

$\Rightarrow a \in \text{QR}_p \Rightarrow \exists b : b^2 \equiv a \pmod{p}$   
we have  $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod{p}$  (using FLT)

$\Leftarrow (\mathbb{Z}_p^*, \cdot)$  is a cyclic group; let  $g$  be its generator  
then  $g^r \equiv a \pmod{p}$  for some **odd**  $r$  (assuming  $a \in \text{QNR}_p$ );  
if  $a^{(p-1)/2} \equiv 1 \pmod{p}$  then  $g^{r(p-1)/2} \equiv 1 \pmod{p}$   
hence  $\text{ord}(g) = (p-1) \mid r(p-1)/2 \Rightarrow r/2$  is an integer,  
i.e.  $r$  is even (a contradiction)

□

# Euler's criterion: testing $a \in \text{QR}_p$ ?

## Lemma 2 (Euler's criterion)

Let  $p > 2$  be a prime and  $a \in \mathbb{Z}_p^*$ . Then  $a \in \text{QR}_p \Leftrightarrow a^{(p-1)/2} \equiv 1 \pmod{p}$ .

Proof.

- $\Rightarrow a \in \text{QR}_p \Rightarrow \exists b : b^2 \equiv a \pmod{p}$   
we have  $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod{p}$  (using FLT)
- $\Leftarrow (\mathbb{Z}_p^*, \cdot)$  is a cyclic group; let  $g$  be its generator  
then  $g^r \equiv a \pmod{p}$  for some **odd**  $r$  (assuming  $a \in \text{QNR}_p$ );  
if  $a^{(p-1)/2} \equiv 1 \pmod{p}$  then  $g^{r(p-1)/2} \equiv 1 \pmod{p}$   
hence  $\text{ord}(g) = (p-1) \mid r(p-1)/2 \Rightarrow r/2$  is an integer,  
i.e.  $r$  is even (a contradiction)

□

## Computing square roots modulo $n = p \cdot q$ (1)

There is a PPT algorithm for factoring  $n \Leftrightarrow$  there is a PPT algorithm for computing square roots modulo  $n$ .

$\Rightarrow$  let's solve  $x^2 \equiv a \pmod{n}$  for  $a \in \text{QR}_n$   
trivially, if  $a \in \text{QR}_n$  then  $a \in \text{QR}_p$  and  $a \in \text{QR}_q$   
compute  $u, v$  such that  $u^2 \equiv a \pmod{p}$ ,  $v^2 \equiv a \pmod{q}$   
use CRT to solve:

$$x \equiv u \pmod{p}$$

$$x \equiv v \pmod{q}$$

trivially,  $x^2 \equiv a \pmod{p}$  and  $x^2 \equiv a \pmod{q}$   
therefore (again by CRT)  $x^2 \equiv a \pmod{n}$

## Computing square roots modulo $n = p \cdot q$ (2)

← let  $a = m^2 \bmod n$  for randomly chosen  $m \in \mathbb{Z}_n^*$   
solve  $x^2 \equiv a \pmod{n}$ ; since  $pq \mid (x - m)(x + m)$  there are four possible solutions:

$$\begin{array}{lll} x \equiv m \pmod{p} & \& x \equiv m \pmod{q} \\ x \equiv m \pmod{p} & \& x \equiv -m \pmod{q} \\ x \equiv -m \pmod{p} & \& x \equiv m \pmod{q} \\ x \equiv -m \pmod{p} & \& x \equiv -m \pmod{q} \end{array}$$

- ▶ computing  $\gcd(x - m, n)$  reveals  $p$  and  $q$  in 2nd and 3rd case, respectively
- ▶ we factor  $n$  with probability  $1/2$  for each choice of  $m$

# Rabin cryptosystem

- ▶ Initialization: choose  $p, q$  large, distinct primes;  $n = p \cdot q$ 
  - ▶ usually choose  $p \equiv q \equiv 3 \pmod{4}$  (★)
  - ▶ easy computation of square roots
  - ▶ encryption is permutation on  $\text{QR}_n$
- ▶ public key:  $n$
- ▶ private key:  $(p, q)$
- ▶ encryption  $E : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ :  $E(m) = m^2 \pmod{n}$ 
  - ▶ fast, just single modular squaring
- ▶ decryption  $D(c)$ :
  - ▶ compute 4 square roots (knowing the factorization, assuming (★)):
$$\pm(c^{(p+1)/4} \pmod{p}) \cdot q \cdot (q^{-1} \pmod{p}) \pm (c^{(q+1)/4} \pmod{q}) \cdot p \cdot (p^{-1} \pmod{q}) \pmod{n}$$
  - ▶ recognize the valid plaintext (context, structure, redundancy etc.)
  - ▶ alternatively, restrict plain/cipher-text space to  $\text{QR}_n$

# Rabin cryptosystem – security (1)

- ▶ CPA scenario: ability to decrypt is provably equivalent to factoring  $n$ 
  - ▶ looks better than RSA
- ▶ insecurity in CCA scenario:
  - ▶ choose random  $m$  and compute  $c = m^2 \bmod n$
  - ▶ use  $c$  as a chosen ciphertext ... let  $m'$  be its decryption
  - ▶ then  $\gcd(m - m', n)$  yields a non-trivial factor of  $n$  with probability  $1/2$
  - ▶ repeat to increase the probability of success
- ▶ padding (for uniqueness of decryption) “destroys” both properties:
  - ▶ equivalence to factoring: because decryption works only on subset of ciphertexts and only the “correct” plaintext is returned
  - ▶ CCA insecurity: small probability of producing a valid ciphertext without knowing the plaintext

## Rabin cryptosystem – security (2)

- ▶ OAEP is a good padding for Rabin
- ▶ some attacks can be “translated” from RSA:
  - ▶ meet in the middle attack on short plaintexts,  $k = k_1 \cdot k_2$ :

$$k^2 \equiv k_1^2 \cdot k_2^2 \pmod{n}$$

- ▶ linearly (polynomially) dependent plaintexts, e.g.  $m_2 = am_1 + b$ :

$$\begin{aligned} (z - m_1) \mid z^2 - c_1 \\ (z - m_1) \mid (az + b)^2 - c_2 \end{aligned} \quad \Rightarrow \quad \gcd(z^2 - c_1, (az + b)^2 - c_2)$$

the computation yields  $z - m_1$  (probably)

- ▶ Example 1:

Let  $n = 77$ ,  $c_1 = 53$ ,  $c_2 = 37$ , and  $m_2 = 2m_1^4 + m_1^2 + 3$ .

$$\begin{aligned} \gcd(z^2 - 53, (2z^4 + z^2 + 3)^2 - 37) &= \\ = \gcd(z^2 + 24, 4z^8 + 4z^6 + 13z^4 + 6z^2 + 49) &= z^2 + 24 = z^2 - 53, \end{aligned}$$

## Rabin cryptosystem – security (2)

- ▶ OAEP is a good padding for Rabin
- ▶ some attacks can be “translated” from RSA:
  - ▶ meet in the middle attack on short plaintexts,  $k = k_1 \cdot k_2$ :

$$k^2 \equiv k_1^2 \cdot k_2^2 \pmod{n}$$

- ▶ linearly (polynomially) dependent plaintexts, e.g.  $m_2 = am_1 + b$ :

$$\begin{aligned} (z - m_1) \mid z^2 - c_1 \\ (z - m_1) \mid (az + b)^2 - c_2 \end{aligned} \quad \Rightarrow \quad \gcd(z^2 - c_1, (az + b)^2 - c_2)$$

the computation yields  $z - m_1$  (probably)

- ▶ Example 2:

Let  $n = 77$ ,  $c_1 = 23$ ,  $c_2 = 58$ , and  $m_2 = 2m_1^3 + m_1^2 + 3$ .

$$\begin{aligned} \gcd(z^2 - 23, (2z^3 + z^2 + 3)^2 - 58) = \\ = \gcd(z^2 + 54, 4z^6 + 4z^5 + 12z^3 + z^4 + 6z^2 + 28) = z + 32 = z - 45, \end{aligned}$$

Thus  $m_1 = 45$  (or  $m_1 = -45 = 32$ ) and  $m_2 = 2 \cdot 45^3 + 45^2 + 3 = 17$  (or  $m_2 = -17 = 60$ ).

## Rabin cryptosystem – security (2)

- ▶ OAEP is a good padding for Rabin
- ▶ some attacks can be “translated” from RSA:
  - ▶ meet in the middle attack on short plaintexts,  $k = k_1 \cdot k_2$ :

$$k^2 \equiv k_1^2 \cdot k_2^2 \pmod{n}$$

- ▶ linearly (polynomially) dependent plaintexts, e.g.  $m_2 = am_1 + b$ :

$$\begin{array}{l} (z - m_1) \mid z^2 - c_1 \\ (z - m_1) \mid (az + b)^2 - c_2 \end{array} \quad \Rightarrow \quad \gcd(z^2 - c_1, (az + b)^2 - c_2)$$

the computation yields  $z - m_1$  (probably)

- ▶ other variants and generalizations ... none of them used in practice