Exercises: RSA, GMR and s^2-mod-n Generator

Software Security

Steffen Helke

Chair of Software Engineering

12th December 2018

Brandenburgische Technische Universität Cottbus - Senftenberg

Objectives of today's exercise

- ➜ Getting to know *how to generate a key pair* for the asymmetric-key cryptosystem *RSA*
- ➜ Being able to perform attacks using *Fermat's factorization method*
- ➜ Being able to apply *s^2-mod-n* generator using *symmetric- and asymmetric-key* variant
- ➜ Getting to know *how to calculate a signature* using *GMR* system

Example for RSA

How to generate a key pair for RSA?

- We assume that the primes $p = 3$ and $q = 13$ are given
- Calculate the secret key d for the given public key $c = 5$

How to generate a suitable RSA key pair?

Exercise for you!

1. Let $p = 3$ and $q = 13$
2. $n =$
3. $\varphi(n) =$
4. Let $c = 5$ with
5. $c \cdot d \equiv$

How to generate a suitable RSA key pair?

Exercise

$$5 \cdot d - k \cdot \quad = 1$$

➜ Calculate d using the *Extended Euclidean algorithm*!

Example for RSA Attack

How to perform an attack using Fermat's factorization method?

- We assume that the key pair is based on module $n = 39$
- Calculate the prime numbers p and q to be able to generate the secret key

Example: Fermat's Factorization Method

$\boxed{\text{Exercise for you!}}$

- Let $n = 39$

$$n = p \cdot q = \underbrace{(a+b)}_{p} \cdot \underbrace{(a-b)}_{q} = a^2 - b^2$$

- Select $a = \lfloor \sqrt{n} + 1 \rfloor =$
- Search for a b to satisfy the equation $n = a^2 - b^2$

➜ $p =$
➜ $q =$

Example for s^2-mod-n Bit Generator

How to encrypt a message using the symmetric-key variant of s^2-mod-n?

- We assume that the primes $p = 7$ and $q = 19$ are given
- Calculate the ciphertext of the plaintext $m = 0110$ for the given initial value $s = 99$

Example: Symmetric-key Variant of s^2-mod-n

Exercise for you!

Given is the following secret key

➜ $n = 133$ with $n = 7 \cdot 19$ and the initial value $s = 99$

Calculating s-sequence **Calculating bit sequence**

Encryption

- Plaintext 0110 is added to the key

Example for s^2-mod-n Bit Generator

How to encrypt a message using the <u>asymmetric-key variant</u> of s^2-mod-n?

- We assume that the primes $p = 7$ and $q = 19$ are given
- Calculate the last bit of the bit sequence for $s_{k+1} = s_5 = 99$

Example for s^2-mod-n asymmetric-key variant

Exercise for you!

Let the secret key

- $n = 133$ with $p = 7$ and $q = 19$
- Further the ciphertext is 0010 and $s_{k+1} = s_5 = 99$

Calculating the last bit of the bit sequence

- $y_p =$
- $y_q =$

Chinese Remainder Algorithm (CRA)

$$CRA\,(y_p, y_q, p, q) =$$

How to combine the intermediate results with CRA?

Extended Euclidean algorithm

$$=$$

$$=$$

$$=$$

In reverse order, i.e. solve all equations to the rest and then insert them step by step

$$=$$

$$=$$

$$=$$

$$=$$

$$=$$

- ➜ We conclude $u =$, $v =$ and $s_4 =$
- ➜ The last bit of the bit sequence is $b_4 =$

Example for Digital Signature System GMR

How to sign a message using GMR?

- We assume that the primes $p = 7$ and $q = 11$ are given
- Calculate the signature s of message $m = 01$ for the reference $R = 17$

➜ We calculate the signature s using the reverse functions of the GMR permutations f_0 and f_1 in the following way $s = f_1^{-1}(f_0^{-1}(17))$

Example: How to create a signature?

Procedure for $f_0^{-1}(17)$

1. Test, whether 17 or -17 is a square, i.e. check $17 \in QR_{77}$
2. Depending on the result in (**1.**)

   calculate roots either for $y = 17$ or for $y = -17$

   $y_7 = y^{\frac{7+1}{4}} \bmod 7$ und $y_{11} = y^{\frac{11+1}{4}} \bmod 11$
3. Combine the intermediate results from (**2.**) with the CRA in such a way that you will get a square again

   $y = CRA(\pm y_7, \pm y_{11}, 7, 11)$
4. Test, whether the result y is within the domain of definition, e.g. $y < \frac{77}{2}$. If not, build the negation of y, e.g. $y = -y \bmod 77$

Step 1: Test, whether 17 is a square

Test for quadratic residue

$17 \in QR_{77} \Leftrightarrow$

Jacobi-Test with Euler's criterion for the primes

-

-

➜ 17 is

Step 2: Calculate the roots of , $\text{mod } p$ and $\text{mod } q$

Formulas

- $y_p = y^{\frac{p+1}{4}} \text{ mod } p$
- $y_q = y^{\frac{q+1}{4}} \text{ mod } q$

Computing the square roots

- $y_7 =$
- $y_{11} =$

➜ Now we have two intermediate results $y_7 =$ and $y_{11} =$

Note

➜ The calculation rule can only be used under the condition $p \equiv q \equiv 3 \text{ mod } 4$!

Step 3: Combine the intermediate results with CRA

Chinese Remainder Algorithm (CRA)

$$CRA(y_p, y_q, p, q) = u \cdot p \cdot y_q + v \cdot q \cdot y_p \mod n$$

Instantiation

$$CRA(\quad,\quad,\quad,\quad) =$$

How to calculate the base vectors u and v?

- The integer variables u and v must fulfill the condition

Step 3: Combine the intermediate results with CRA

Extended Euclidean algorithm

$$=$$

$$=$$

$$=$$

In reverse order, i.e. solve all equations to the rest and then insert them step by step

$$=$$

$$=$$

$$=$$

$$=$$

$$=$$

- ➜ The base vectors are $u =$ and $v =$
- ➜ Results in $CRA(\quad , \quad , 7, 11) =$
- ➜ **Note**: In addition, check whether the root

Step 3 & 4: Test, whether 37 is a square and $37 \in D_{77}$

Test for quadratic residue

$$37 \in QR_{77} \Leftrightarrow$$

Jacobi-Test with Euler's criterion for the primes

- for $p = 7$

- for $p = 11$

Example: How to create a signature?

Procedure for $f_1^{-1}(37)$

1. Test, whether $\frac{37}{4}$ is square, i.e. check $\frac{37}{4} \in QR_{77}$, Note the division is a multiplication with the inverse of 4, i.e. $\frac{37}{4} = 37 \cdot 4^{-1} \bmod 77$
2. Depending on the result in (**1.**)

   calculate roots either for $y = \frac{37}{4}$ or for $y = \frac{-37}{4}$

   $y_7 = y^{\frac{7+1}{4}} \bmod 3$ und $y_{11} = y^{\frac{11+1}{4}} \bmod 7$
3. Combine the intermediate results from (**2.**) with the CRA in such a way that you will get a square again

   $y = CRA\,(\pm y_7, \pm y_{11}, 7, 11)$
4. Test, whether the result y is within the domain of definition, e.g. $y < \frac{77}{2}$. If not, build the negation of y, e.g. $y = -y \bmod 77$

Step 1: Test, whether $\frac{37}{4}$ is a square

Test for quadratic residue

- $\frac{37}{4} \in QR_{77}$

How to calculate the multiplicative inverse of 4?

- The multiplicative inverse i has to fulfill ...

Test using the multiplicative inverse

- $\frac{37}{4} = 37 \cdot 4^{-1} =$

Step 2: Calculate the roots of 67, $\bmod p$ and $\bmod q$

Formulas

- $y_p = y^{\frac{p+1}{4}} \bmod p$
- $y_q = y^{\frac{q+1}{4}} \bmod q$

Computing the square roots for the primes

-
-

➜ Now we have two intermediate results $y_7 =$ and $y_{11} =$

Note

➜ The calculation rule can only be used under the condition $p \equiv q \equiv 3 \bmod 4$!

Step 3 & 4: Combine the intermediate results with CRA

Chinese Remainder Algorithm (CRA)

$$CRA(y_p, y_q, p, q) = u \cdot p \cdot y_q + v \cdot q \cdot y_p \mod n$$

$$CRA(\quad, \quad, 7, 11) =$$

The base vectors u and v are ...

$$CRA(\quad, \quad, 7, 11) =$$

Test for quadratic residue and check for domain

Conclusion: $f_1^{-1}(f_0^{-1}(17)) =$, i.e. the signature of $m = 01$ is