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?

1. Let $p = 3$ and $q = 13$
2. $n = p \cdot q = 39$
3. $\varphi(n) = (p - 1) \cdot (q - 1) = 24$
4. Let $c = 5$ with $ggT(5, 24) = 1$
5. $c \cdot d - k \cdot \varphi(n) = 1 = ggT(c, \varphi(n))$
6. $5 \cdot d - k \cdot 24 = 1 = ggT(5, 24)$

   ➜ Calculate d using the *Extended Euclidean algorithm*!

How to generate a suitable RSA key pair?

Exercise

$5 \cdot d - k \cdot 24 = 1 = ggT(5, 24)$

➜ Calculate d using the *Extended Euclidean algorithm*!

$$24 = 4 \cdot 5 + 4 \qquad 4 = 24 - 4 \cdot 5$$
$$5 = 1 \cdot 4 + 1 \qquad 1 = 5 - 1 \cdot 4$$

$$\begin{aligned} 1 &= 5 - 1 \cdot 4 \\ &= 5 - 1 \cdot (24 - 4 \cdot 5) \\ &= 5 \cdot 5 - 1 \cdot 24 \end{aligned}$$

$c \cdot d - k \cdot \phi(n) = 1$
$\Rightarrow d = 5$

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

- Let $n = 39$

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

- Select $a = \lfloor \sqrt{n} + 1 \rfloor = \lfloor \sqrt{39} + 1 \rfloor = 7$
- Search for a b to satisfy the equation $n = a^2 - b^2$
- $b^2 = a^2 - n = 7^2 - 39 = 10$
  - ➜ 10 is not a square! $\Rightarrow$ Increase a by 1
- $b^2 = a^2 - n = 8^2 - 39 = 25$
  - ➜ 25 is a square!
- if $a = 8$ and $b = 5$ we obtain for p and q
  - ➜ $p = a + b = 8 + 5 = 13$
  - ➜ $q = a - b = 8 - 5 = 3$

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

Given is the following secret key

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

Calculating *s*-sequence

$$
\begin{aligned}
s_0 &= 99^2 \equiv 92 \bmod 133 \\
s_1 &= 92^2 \equiv 85 \bmod 133 \\
s_2 &= 85^2 \equiv 43 \bmod 133 \\
s_3 &= 43^2 \equiv 120 \bmod 133 \\
s_4 &= 120^2 \equiv 36 \bmod 133 \\
s_5 &= 36^2 \equiv 99 \bmod 133
\end{aligned}
$$

Calculating bit sequence

$$
\begin{aligned}
b_0 &= 92 \equiv 0 \bmod 2 \\
b_1 &= 85 \equiv 1 \bmod 2 \\
b_2 &= 43 \equiv 1 \bmod 2 \\
b_3 &= 120 \equiv 0 \bmod 2 \\
b_4 &= 36 \equiv 0 \bmod 2 \\
b_5 &= 99 \equiv 1 \bmod 2
\end{aligned}
$$

Encryption

- Plaintext 0110 is added to the Bit-sequence 0110 by XOR
  ➜ We obtain the ciphertext 0000

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 s²-mod-n asymmetric-key variant

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

- $y_p = y^{\frac{p+1}{4}} = 99^{\frac{7+1}{4}} = 99^2 \equiv 1 \mod 7$
- $y_q = y^{\frac{q+1}{4}} = 99^{\frac{19+1}{4}} = 99^5 \equiv 17 \mod 19$

Chinese Remainder Algorithm (CRA)

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

$$CRA\,(1, 17, 7, 19) = u \cdot 7 \cdot 17 + v \cdot 19 \cdot 1 \mod 133$$

➜ To find u and v we need to solve $u \cdot p + v \cdot q = 1$ by the *Extended Euclidean algorithm*

How to combine the intermediate results with CRA?

Extended Euclidean algorithm

$$19 = 2 \cdot 7 + 5 \qquad (q = s_1 \cdot p + r_1)$$

$$7 = 1 \cdot 5 + 2 \qquad (p = s_2 \cdot r_1 + r_2)$$

$$5 = 2 \cdot 2 + 1 \qquad (r_1 = s_3 \cdot r_2 + r_3)$$

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

$$1 = 5 - 2 \cdot 2 \qquad (r_3 = r_1 - s_3 \cdot r_2)$$

$$1 = 5 - 2 \cdot (7 - 1 \cdot 5) \qquad (r_3 = r_1 - s_3 \cdot (p - s_2 \cdot r_1))$$

$$1 = 3 \cdot 5 - 2 \cdot 7 \qquad (r_3 = 3 \cdot r_1 - 2 \cdot p)$$

$$1 = 3 \cdot (19 - 2 \cdot 7) - 2 \cdot 7 \qquad (r_3 = 3 \cdot (q - s_1 \cdot p) - 2 \cdot p))$$

$$1 = 3 \cdot 19 - 8 \cdot 7 \qquad (r_3 = 3 \cdot q - 8 \cdot p)$$

➜ We conclude $u = -8$, $v = 3$ and $s_4 = CRA(1, 17, 7, 19) = 36$

➜ The last bit of the bit sequence is $b_4 = (s_4 \bmod 2) = 0$

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

$$17 \in QR_{77} \Leftrightarrow 17 \in QR_7 \wedge 17 \in QR_{11}$$

Jacobi-Test with Euler's criterion

- for $p = 7$ we obtain $\left(\frac{17}{7}\right) = 17^{\frac{7-1}{2}} = 17^3 \equiv -1 \mod 7$
  $\Rightarrow 17 \notin QR_7$
- for $q = 11$ we obtain $\left(\frac{17}{11}\right) = 17^{\frac{11-1}{2}} = 17^5 \equiv -1 \mod 11$
  $\Rightarrow 17 \notin QR_{11}$

➜ 17 is not a quadratic residue, i.e. $17 \notin QR_{77}$

➜ However a square test for $-17 \equiv 60 \mod 77$ is successful.
Hence we use in the following 60 to calculate the square root!

Step 2: Calculate the roots of 60, mod p and mod q

Formulas

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

Computing the square roots

- $y_7 = 60^{\frac{7+1}{4}} = 60^2 = 2 \mod 7$
- $y_{11} = 60^{\frac{11+1}{4}} = 60^3 = 4 \mod 11$

➜ Now we have two intermediate results $y_7 = 2$ and $y_{11} = 4$

Note

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

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

$$CRA\,(2, 4, 7, 11) = u \cdot 7 \cdot 4 + v \cdot 11 \cdot 2 \mod 21,$$

How to calculate the base vectors u and v?

- The integer variables u and v must fulfill the condition
  $u \cdot 7 + v \cdot 11 = 1$
- Values for u and v can be calculated using the *Extended Euclidean algorithm*

Step 3: Combine the intermediate results with CRA

Extended Euclidean algorithm

$$11 = 1 \cdot 7 + 4 \qquad (q = s_1 \cdot p + r_1)$$
$$7 = 1 \cdot 4 + 3 \qquad (p = s_2 \cdot r_1 + r_2)$$
$$4 = 1 \cdot 3 + 1 \qquad (r_1 = s_3 \cdot r_2 + r_3)$$

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

$$1 = 4 - 1 \cdot 3 \qquad (r_3 = r_1 - s_3 \cdot r_2)$$
$$1 = 4 - 1 \cdot (7 - 1 \cdot 4) \qquad (r_3 = r_1 - s_3 \cdot (p - s_2 \cdot r_1))$$
$$1 = 2 \cdot 4 - 1 \cdot 7 \qquad (r_3 = 2 \cdot r_1 - 1 \cdot p)$$
$$1 = 2 \cdot (11 - 1 \cdot 7) - 1 \cdot 7 \qquad (r_3 = 2 \cdot (q - s_1 \cdot p) - 1 \cdot p))$$
$$1 = 2 \cdot 11 - 3 \cdot 7 \qquad (r_3 = 2 \cdot q - 3 \cdot p)$$

- ➜ The base vectors are $u = -3$ and $v = 2$
- ➜ Results in $CRA(2, 4, 7, 11) = -3 \cdot 7 \cdot 4 + 2 \cdot 11 \cdot 2 \equiv 37 \bmod 77$
- ➜ **Note**: In addition, check whether the root 37 is a square again

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

Test for quadratic residue

$$37 \in QR_{77} \Leftrightarrow 37 \in QR_7 \wedge 37 \in QR_{11}$$

Jacobi-Test with Euler's criterion

- for $p = 7$ we obtain $\left(\frac{37}{7}\right) = 37^{\frac{7-1}{2}} = 37^3 \equiv 1 \mod 7$
  $\Rightarrow 37 \in QR_7$
- for $q = 11$ we obtain $\left(\frac{37}{11}\right) = 37^{\frac{11-1}{2}} = 37^5 \equiv 1 \mod 11$
  $\Rightarrow 37 \in QR_{11}$

➜ 37 is a quadratic residue, i.e. $37 \in QR_{77}$

Check the condition $37 \in D_{77}$

$$37 < \frac{77}{2} \Leftrightarrow 37 < 38,5$$

➜ 37 is within the definition range, i.e. $f_0^{-1}(17) = 37$

➜ Next step is to calculate $f_1^{-1}(37)$ to obtain the complete signature

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

- $\frac{37}{4} \in QR_{77} \Leftrightarrow \frac{37}{4} \in QR_7 \wedge \frac{37}{4} \in QR_{11}$

How to calculate the multiplicative inverse of 4?

- The multiplicative inverse i has to fulfill the following condition $i \cdot 4 + n \cdot 77 = 1$
- We solve this by the *Extended Euclidean algorithm*
  $77 = 19 \cdot 4 + 1 \;\rightarrow\; 1 = 1 \cdot 77 - 19 \cdot 4 \;\rightarrow\; i = 4^{-1} = -19 \equiv 58 \bmod 77$

Test using the multiplicative inverse

- $\frac{37}{4} = 37 \cdot 4^{-1} = 37 \cdot 58 \equiv 67 \bmod 77 \rightarrow 67 \in QR_{77} \Leftrightarrow 67 \in QR_7 \wedge 67 \in QR_{11}$
- $\left(\frac{67}{7}\right) = 67^{\frac{7-1}{2}} = 67^3 \equiv 1 \mod 7 \rightarrow 67 \in QR_7$
- $\left(\frac{67}{11}\right) = 67^{\frac{11-1}{2}} = 67^5 \equiv 1 \mod 11 \rightarrow 67 \in QR_{11}$

Conclusion: $\frac{37}{4} \in QR_{77}$ because $67 \in QR_{77}$

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

Formulas

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

Computing the square roots

- $y_7 = 67^{\frac{7+1}{4}} = 67^1 = 2 \mod 7$
- $y_{11} = 67^{\frac{11+1}{4}} = 67^2 = 1 \mod 11$

➜ Now we have two intermediate results $y_7 = 2$ and $y_{11} = 1$

Note

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

Step 3 & 4: Combine the intermediate results with CRA

Chinese Remainder Algorithm (CRA)

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

$$CRA\,(2, 1, 7, 11) = u \ \cdot 7 \cdot 1 + v \ \cdot 11 \cdot 2 \mod 77,$$

The base vectors u and v are already known

$$CRA\,(2, 1, 7, 11) = -3 \ \cdot 3 \cdot 1 + 2 \ \cdot 7 \cdot 1 \equiv 23 \mod 77,$$

➜ Finally we need to check, whether 23 is a square

Test for quadratic residue

- $23 \in QR_{77} \Leftrightarrow 23 \in QR_7 \wedge 23 \in QR_{11}$
- $\left(\frac{23}{7}\right) = 23^{\frac{7-1}{2}} = 23^3 \equiv 1 \mod 3$ ➜ $23 \in QR_7$
- $\left(\frac{23}{11}\right) = 23^{\frac{11-1}{2}} = 23^5 \equiv 1 \mod 3$ ➜ $23 \in QR_{11}$
- We conclude $23 \in QR_{77}$, further $23 \in D_{77}$, because $23 < \frac{77}{2}$

Conclusion: $f_1^{-1}(f_0^{-1}(17)) = 23$, i.e. the signature of $m = 01$ is 23