RESIDUE NUMBER SYSTEM & CHINESE REMAINDER THEOREM

[Publish Date]

European Cyber Security Challenge 2019
Bucharest, Romania

1. Initial Write-Up

Description:

The Chinese Remainder Theorem (CRT) is used in various cryptographic applications in order to speed up calculations, for instance in the RSA algorithm [1]. The goal of this task is to understand the discrete mathematics that form the basis of modern cryptography by using Euler's Theorem, Fermat Little Theorem, CRT and by solving linear congruent relationships.

2. Challenge specifications

- Category: Crypto
- Difficulty : Easy
- Expected time to solve: 1h

3. Technical specifications

- Recommended use of SAGE: http://www.sagemath.org/

4. Questions and answers

1. The Residue Number System (RNS) [2] allows for parallel computations by splitting a number into residues of smaller moduli. You are given the number N = (5619; 181876; 5608477) in RNS format with base elements (198247; 427363; 8125766).
    a. Is this a proper RNS basis?

b. What is this number in binary format?

Solution:

a. Yes, this is a proper basis, because the basis elements are coprime - check gcd with a tool. For instance, in Sage, we can do:

gcd(198247; 427363) == 1; gcd(198247; 8125766) == 1; gcd(427362; 8125766) == 1

which all evaluate to True.

b. The number in binary is n = 184375329. To and this, we have to solve the congruence relations: n ≡ 5619 (mod 198247); n ≡181876 (mod 427363); n ≡5608477(mod 8125766).

From Sage we get:

crt(5608477,181876, 8125766,427363) = n=184375329,

crt(5619,181876,198247,427363) = n=184375329

2. Compute the two least significant digits of 2019^{2019} "by hand" without help of a mathematical software tool. Hint: Recall Euler's theorem: If gcd(a; n) = 1 then a-(n) ≡1 (mod n).

Solution:

We need to compute 2019^{2019}(mod 100)(1). We'll do that by using number theory and not a tool to solve it directly. We know that, 100 = 25 ▪ 4 and gcd (25, 4) = 1, so by CRT (1) is equivalent to solving x ≡2019^{2019} (mod 25); x ≡ 2019^{2019} (mod 4).

We have that ϕ(25) = 20 and ϕ (4) = 2. Therefore, x ≡2019^{2019} (mod 25) → x ≡ $\left(2019^{\phi(25)}\right)^{100+19}$ (mod 25) → x ≡ 2019^{2019} (mod 25)

x^{2019}(mod 25) → x ≡19^{19}(mod 25) → x ≡ ▪$19^{\phi(25)}$▪ 19^{-1} (mod 25)

→ x ≡ 19^{-1} (mod 25) → x ≡4 (mod 25).

And

x ≡ 20192019 (mod 4) → x ≡ (2019-(4))1009+1 (mod 4) → x ≡ 20191 (mod 4) → x ≡ 3(mod 4)

We need to solve the following system of equivalence relations:

$$\begin{cases} x \equiv 4 \ (mod\ 25) \\ x \equiv 3 \ (mod\ 4) \ \rightarrow \ x = 4j + 3 \end{cases}$$

$$\begin{cases} 4j + 3 \equiv 4 \ (mod\ 25) \rightarrow \quad 4j \equiv 1 \ (mod\ 25) \rightarrow \quad j \equiv 19 \\ x = 4 \cdot 19 + 3 \rightarrow x = 79 \end{cases}$$

Sage code verifcation:

crt(4,3,25,4)

euler_phi(25)

mod(2019,2)

inverse_mod(19,25)

3. Suppose that Alice wants to send the same secret message m to Bob, Chris and Dona. The public modulus of these three people is given by the numbers n_B = 699; n_C= 3205 and n_D= 8309, and they all have the same public exponent e = 13. If the transmitted cipher texts are C_B= 670, C_C= 2574, C_D= 5380 respectively, and the message m (with the help of the Chinese Remainder Theorem).

Solution:

Hint: The messages that Alice will transmit are C_B= m^{13} (mod n_B) for Bob, C_C= m^{13} (mod n_C) for Chris and C_D = = m^{13} (mod n_D) for Dona.

If we give the hint, the exercise difficulty reduces.

Calculate the cipher texts for verification.Make sure the numbers are coprime

gcd(699,3205)

gcd(3205,8309)

gcd(699,8309)

Calculate the ciphertexts for verification

a = mod(4^{13}, 233 * 3); a a = 670

b = mod(4^{13}, 3205); b b = 2574

c = mod(4^{13}, 8309); c c = 5380

Compute CRT for all 3 sets of numbers

crt(670,2574,699,3205) give 2140309, 699 *3205 = 2240295

crt(5380,2140309,8309,2240295) that gives 67108864 final CRT value

Compute message m from log

$m = \frac{\log(67108864)}{13} \rightarrow$ m = 2log(2), from which we can conclude that m = 4.

5. Attack Scenario

N/A

6. Installation instructions

N/A

7. Tools needed

- Sage (http://www.sagemath.org/)

8. Artefacts Provided

N/A

9. Walkthrough (writeup)

N/A

10. References

1. RSA with CRT https://en.wikipedia.org/wiki/RSA_(cryptosystem),https://www.di-mgt.com.au/crt_rsa.html
2. Residue Number System https://en.wikipedia.org/wiki/Residue_number_system,https://web.stanford.edu/class/ee486/doc/chap2.pdf
3. Chinese Remainder Theorem https://brilliant.org/wiki/chinese-remainder-theorem/ , http://gauss.math.luc.edu/greicius/Math201/Fall2012/Lectures/ChineseRemainderThm.

article.pdf