CS 70 Discrete Mathematics and Probability Theory
Summer 2018 Sinho Chewi and Vrettos Moulos DIS 2D

1 Baby Fermat

Assume that a does have a multiplicative inverse mod m. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions.

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

Solution:

(a) There are only m possible values mod m, and so after the m-th term we should see repetitions.

(b) We will temporarily use the notation a^* for the multiplicative inverse of a to avoid confusion. If we multiply both sides by $(a^*)^j$ in the third line below, we get

$$\begin{aligned}
a^i &\equiv a^j & \pmod{m},\\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}} & \pmod{m},\\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} & \pmod{m},\\
a^{i-j} &\equiv 1 & \pmod{m}.
\end{aligned}$$

(c) We can rewrite $a^{i-j} \equiv 1 \pmod{m}$ as $a^{i-j-1}a \equiv 1 \pmod{m}$. Therefore a^{i-j-1} is the multiplicative inverse of $a \pmod{m}$.

2 RSA Practice

Consider the following RSA schemes and solve for asked variables.

(a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key d? Calculate the exact value.

(b) If the receiver gets 4, what was the original message?

(c) Encode your answer from part (**??**) to check its correctness.

Solution:

(a) The private key d is defined as the inverse of $e \pmod{(p-1)(q-1)}$. Thus we need to compute $9^{-1} \bmod (5-1)(11-1) = 9^{-1} \bmod 40$. Find inverse of e mod $(5-1)(11-1) = 40$. Compute $\text{egcd}(40,9)$:

$$\begin{aligned} \text{egcd}(40,9) &= \text{egcd}(9,4) && [4 = 40 \bmod 9 = 40-4(9)] \\ &= \text{egcd}(4,1) && [1 = 9 \bmod 4 = 9-2(4)]. \\ 1 &= 9-2(4). \\ 1 &= 9-2(40-4(9)) \\ &= 9-2(40)+8(9) = 9(9)-2(40). \end{aligned}$$

We get $-2(40)+9(9) = 1$. So the inverse of 9 is 9. So $d = 9$.

(b) 4 is the encoded message. We can decode this with $D(m) \equiv m^d \equiv 4^9 \equiv 14 \pmod{55}$. $4^9 \equiv 14 \pmod{55}$. Thus the original message was 14.

(c) The answer from the second part was 14. To encode the number x we must compute $x^e \bmod N$. Thus, $14^9 \equiv 14 \cdot (14^2)^4 \equiv 14 \cdot (31^2)^2 \equiv 14 \cdot (26^2) \equiv 14 \cdot 16 \equiv 4 \pmod{55}$. This verifies the second part since the encoded message was suppose to be 4.

3 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p,q,r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod N$.

Solution:

$N = pqr$ where p,q,r are all prime. Then, let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N,e) and calculate $d = e^{-1} \bmod (p-1)(q-1)(r-1)$. People who wish to send me a secret, x, send $y = x^e \bmod N$. I decrypt an incoming message, y, by calculating $y^d \bmod N$.

Does this work? We prove that $x^{ed} - x \equiv 0 \pmod N$ and thus $x^{ed} \equiv x \pmod N$. To prove that $x^{ed} - x \equiv 0 \pmod N$, we factor out the x to get $x \cdot (x^{ed-1} - 1) = x \cdot (x^{k(p-1)(q-1)(r-1)+1-1} - 1)$ because $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$. As a reminder, we are considering the number: $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$.

We now argue that this number must be divisible by p, q, and r. Thus it is divisible by N and $x^{ed} - x \equiv 0 \pmod N$.
To prove that it is divisible by p:

- If x is divisible by p, then the entire thing is divisible by p.

- If x is not divisible by p, then that means we can use FLT on the inside to show that $(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{p}$. Thus it is divisible by p.

The same reasoning shows that it is divisible by q and r.

4 RSA with Limited Messages

Suppose that Alice only has two possible messages she might send Bob: either "Yes" or "No".

(a) If Alice and Bob use the standard RSA procedure, describe how Eve could find out which message Alice sent.

(b) Describe how Alice and Bob might modify the RSA procedure to stop Eve from using this exploit. *(Hint: Try using a one-time pad somewhere in your procedure)*

Solution:

(a) Since there are only two messages Alice might have encrypted, Eve can just try both. Specifically, since Eve also knows Bob's public key, she can use it to encrypt both the message "Yes" and the message "No". Whichever encryption matches the encrypted message Alice sent must be the plaintext message Alice wanted to get to Bob.

(b) We would ideally like to just use the one-time pad procedure discussed in lecture. Even with only two possible messages, Eve gets absolutely no information about the original message if all she sees is the message xor-ed with an unknown pad. However, in order to make this work, we need a way for both Alice and Bob to know the pad without letting Eve find out.

This is where we leverage the original RSA procedure. We can have Alice pick a pad randomly, then encrypt the pad (rather than her message!) using Bob's public key and send it to Bob. Since Alice could have chosen any appropriate-length bit string for the pad, Eve can't use the trick from the previous part to find out the pad. This means that Alice and Bob can now use the one-time pad procedure to send Alice's actual message without worrying about Eve exploiting the fact that there are only two possible messages.