CS 70 Discrete Mathematics and Probability Theory
Fall 2025 Sabin, Hug

HW 05

Due: Saturday, 10/5, 4:00 PM
Grace period until Saturday, 10/5, 6:00 PM
Remember to show your work for all problems!

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.) If you used an LLM, place transcripts of your chats here.

1 RSA Practice

Note 7

Consider the following RSA scheme and answer the specified questions.

(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) Encrypt your answer from part (b) to check its correctness.

2 RSA with CRT

Note 7

Inspired by the efficiency of solving systems of modular equations with CRT, Bob decides to use CRT to speed up RSA!

He first generates the public key (e,N) and private key d as normal, keeping track of the primes $pq = N$. Recall that e is chosen to be coprime to $(p-1)(q-1)$, and d is then defined as $e^{-1} \pmod{(p-1)(q-1)}$. Next, he stores the following values:

$$\begin{aligned} d_p &\equiv d \pmod{p-1} \\ d_q &\equiv d \pmod{q-1} \end{aligned}$$

After receiving an encrypted message $c = m^e \pmod{N}$ from Alice, Bob computes the following expressions:

$$x \equiv c^{d_p} \pmod{p}$$
$$x \equiv c^{d_q} \pmod{q}$$

The message m then calculated as the solution to the above modular system.

(a) Show that this algorithm is correct, i.e. that $x \equiv m$ is the only solution $\pmod{N}$ to the above modular system.

(b) Emboldened by his success in using CRT for RSA, Bob decides to invent a new cryptosystem. To generate his keypair, he first generates $N = pq$. Then, he chooses three numbers g, r_1, r_2 ($q \nmid g$ and $p \nmid g$) and publishes the public key $(N, g_1 = g^{r_1(p-1)} \pmod{N}, g_2 = g^{r_2(q-1)} \pmod{N})$. His private key is (p, q).

To encrypt a message, Alice chooses two numbers s_1, s_2 and sends $c_1 = mg_1^{s_1}, c_2 = mg_2^{s_2}$.

Bob decrypts this message by solving the modular system

$$x \equiv c_1 \pmod{p}$$
$$x \equiv c_2 \pmod{q}$$

Show that this algorithm is correct, i.e. show that $x \equiv m$ is the only solution $\pmod{N}$ to the above modular system.

(c) This system is woefully insecure. Show how anyone with access to the public key can recover p, q, given that $g_1 \not\equiv 1 \pmod{q}$.

3 Tweaking RSA

Note 7

You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

(a) Show how you choose $e, d > 1$ in the encryption and decryption function, respectively. Prove the correctness property: the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve now compute d in the decryption function? If so, by what algorithm?

(c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain the modifications made to encryption and decryption and include a proof of correctness showing that $D(E(x)) = x$.

4 Equivalent Polynomials

Note 7
Note 8

This problem is about polynomials with coefficients in $\mathrm{GF}(p)$ for some prime $p \in \mathbb{N}$. We say that two such polynomials f and g are *equivalent* if $f(x) \equiv g(x) \pmod{p}$ for every $x \in \mathrm{GF}(p)$.

(a) Show that $f(x) = x^{p-1}$ and $g(x) = 1$ are **not** equivalent polynomials under $\mathrm{GF}(p)$.

(b) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 13 that is equivalent to $f(x) = x^{13}$ over $\mathrm{GF}(13)$; then find a polynomial with degree strictly less than 7 that is equivalent to $g(x) = 2x^{74} + 6x^7 + 3$ over $\mathrm{GF}(7)$.

(c) In $\mathrm{GF}(p)$, prove that whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

5 Lagrange's Residents

Note 8

A group of humans has settled at the Earth–Moon L5 point, a Lagrange Point near earth. They have a message for their friends on Earth, and its your job to decode it.

A four packet message is sent using a degree 3 polynomial $P(x)$, where $P(0) = m_1$, $P(1) = m_2$, $P(2) = m_3$, and, $P(3) = m_4$. $P(4)$ and $P(5)$ are also sent.

Unfortunately, the channel lost $P(0)$ and $P(3)$, so the earthlings only received:

$(1,3),(2,7),(4,-90),(5,-335)$

Using Lagrange interpolation and a graphical calculator (eg. Desmos), recover $P(0)$ and $P(3)$ to unlock the space explorers' message.