W202 - Homework 1

Problem 1a : What does Bob send Alice?

$e = 3$ (Bob's public key)
$N = 1081$
$m = 13$ (Alice's message)

Solution : Use RSA encryption algorithm to encrypt Alice's message using Bob's public key.

Step 1 : Calculate "c", given values "e", "N", "m".

↳ $c = m^e \bmod n$ (RSA encryption algorithm)
↳ $c = 13^3 \bmod 1081$ (substitute m, e, n variables)
↳ $c = 2197 \bmod 1081$ (calculate 13^3)
↳ $\underline{c = 35}$ (calculate 2197 mod 1081) using WolframAlpha

Answer : Alice sends ciphertext "35" to Bob.

Problem 1b : Show Bob decrypting message.

$d = 675$ (Bob's decryption key)

$N = 1081$

$c = 35$ (Ciphertext from problem 1a)

Solution : Use RSA decryption algorithm to decrypt Alice's message with Bob's private key.

Step 1 : Calculate "m", given values "c", "d", "n".

↳ $m = c^d \bmod n$ (RSA decryption algorithm)

↳ $m = 35^{675} \bmod 1081$ (substitute c, d, n variables)

↳ $m = 13$ (used WolframAlpha to calculate m)

Answer : Yes. When Bob decrypts ciphertext "35" from Alice, he gets "13" which is the origin message from Alice.

Problem 2a: Encode "hi" using scheme.

Following the text-to-number encoding scheme...

01	02	03	04	05	06	07	08	09
↓	↓	↓	↓	↓	↓	↓	↓	↓
a	b	c	d	e	f	g	h	i
10	11	12	13	14	15	16	17	18
↓	↓	↓	↓	↓	↓	↓	↓	↓
j	k	l	m	n	o	p	q	r
19	20	21	22	23	24	25	26	
↓	↓	↓	↓	↓	↓	↓	↓	
s	t	u	v	w	x	y	z	

Solution: Find encoding for "h" an "i".

↳ h → 08 (encoding for "h" and "i")
i → 09

↳ 08 09 (combined encoding of "hi")

↳ 809 (encoding after removing spaces)

Answer: "hi" encoded with scheme is:

↳ 0809 (combined without spaces removed)

↳ 809 (combined with spaces removed)

Problem 2b : What does Alice send Bob?

$e = 7$ (Bob's public key)

$p = 1003001$

$q = 1000033$

$m = 809$ (from problem 2a)

Solution : Use RSA encryption algorithm to encrypt Alice's message "hi" before sending to Bob.

$$\underbrace{C}_{\text{ciphertext}} = \underbrace{m}_{\text{message}}^{\overbrace{e}^{\text{encryption key}}} \bmod \underbrace{n}_{p \cdot q}$$

(RSA encryption algorithm)

Step 1 : Solve for "n", given values for "p" & "q".

↳ $n = p \cdot q$

↳ $n = (1003001)(1000033)$

↳ $n = 1003034099033$

(calculate value n given p and q)

Step 2 : Calculate "c", given values "m", "e", "n".

↳ $C = 809^7 \bmod 1003034099033$

↳ $C = 253100088695$

(calculate value c using WolframAlpha)

$$\boxed{\text{Answer : Alice sends "253100088695" as ciphertext to Bob.}}$$

Problem 2c:

Question: What algorithm would Bob use to calculate his decryption key "d"?

$\boxed{\text{Answer : Extended Euclidean Algorithm}}$

More specifically, referring to the RSA equation "$e \cdot d \bmod \phi(n) = 1$", where "d" is the decryption key, we can use the Extended Euclidean Algorithm to solve for "d". The equation can be written as:

$$\text{"} \phi(n)(v) + e(y) = 1 \text{"},$$

where the resulting value of (y) is the the corresponding value of decryption key "d". An alternative equation can be derived from re-writing "$e \cdot d \bmod \phi(n) = 1$" to "$d = e^{-1} \bmod \phi(n)$", which will also calculate the decryption value "d".

Problem 2d:

Part 1: show $d = 71645149 7143$.

Solution: Solve for "d" using RSA equation.

$e = 7$ (Bob's public key)

$p = 1003001$

$q = 1000033$

RSA equations for "d": $d = e^{-1} \bmod \phi(n)$
(from problem 2c)

Step 1: Find $\phi(n)$ given values "p" and "q".

↳ $\phi(n) = (p-1)(q-1)$

↳ $\phi(n) = (1003001-1)(1000033-1)$

↳ $\phi(n) = (1003000)(1000032)$

↳ $\phi(n) = 1003032096000$

Step 2: Use RSA equation to solve for "d".

↳ $e \cdot d \bmod \phi(n) = \underline{1}$ (RSA equation)

↳ $d = e^{-1} \bmod \phi(n)$ (RSA rewritten to find "d")

↳ $d = 7^{-1} \bmod 1003032096000$ (Calculated using WolframAlpha)

↳ $d = 716451497143$

$\boxed{\text{Answer (part 1): Yes. The decryption key is valid.}}$

Problem 2d :

part 2 : Decrypt Alice's message.

Solution : Use RSA decryption algorithm.

$d = 7164514974 3$ (Bob's decryption key)

$n = 100303409903 3$ (from problem 2b)

$c = 25310008869 5$ (from problem 2b)

$$\underbrace{m}_{\text{message}} = \underbrace{c}_{\text{ciphertext}}^{\overbrace{d}^{\text{decryption key}}} \bmod \underbrace{n}_{p \cdot q \text{ (RSA)}} \quad \text{(RSA decryption formula)}$$

Step 1 : Solve for "m", given values "c", "d", "n".

$\hookrightarrow m = 253100088695^{7164514974 3} \bmod 1003034099033$

$\hookrightarrow \underline{\underline{m = 809}}$ (Calculated using WolframAlpha)

Answer (part 2 : Yes. Bob was able to decrypt Alice's message "809" using his decryption key "d".

Problem 3 :

Explain why $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$
and not $e \cdot d \equiv 1 \pmod{(pq)}$

Answer :

The RSA algorithm utilizes properties of inverses in order to encrypt and decrypt a message. More specifically, the RSA equation "$m^{ed} \bmod n$" shows that the encryption exponent "e" and decryption exponent "d" are modular inverses of eachother, derived from a special group of integers. Using the RSA equation "$m^{ed} \bmod n$" and the Fermat-Euler Theorem "$a^{\phi(n)} \equiv 1 \bmod n$", we can mathematically prove the equations :

$e \cdot d \equiv 1 \bmod (p-1)(q-1)$ is true and,
$e \cdot d \equiv 1 \bmod (pq)$ is not true.

(see next page)

Proof 1 : If $m^{ed} \bmod n$, and
$e \cdot d \equiv 1 \bmod (p-1)(q-1)$, then :

↳ $m^{ed} \bmod n$ (RSA equation)

↳ $m^{k(p-1)(q-1)+1} \bmod n$ (1 mod $\phi(n)$ ≈ $1 + k\phi(n)$ property)

↳ $m^{k(\phi n)+1} \bmod n$ ($(p-1)(q-1) \approx \phi(n)$)

↳ $(m^1)(m^{\phi(n)})^k \bmod n$ (Distributive Property)

↳ $(m^1)(1)$ (Reduce with Euler theorem)

≈ $\underline{\underline{m}}$ Answer: As the original message can be recovered, the equation $e \cdot d \equiv 1 \bmod (p-1)(q-1)$ is true.

Proof 2 : If $m^{ed} \bmod n$, and
$e \cdot d \equiv 1 \bmod (pq)$, then :

↳ $m^{ed} \bmod n$ (RSA equation)

↳ $m^{k(pq)+1} \bmod n$ (Cannot factor further)

\# As we cannot factor equation further, we are unable to prove that equation "$e \cdot d \equiv 1 \bmod (pq)$" is true. #

Problem 4 :

Prove "m" is prime if and only if $\phi(m) = m-1$.

Proof # 1 : If m is prime, then $\phi(m) = m-1$.

↳ Euler's Totient Function $\phi(m)$ counts the number of positive integers up to "m", that are co-prime to "m".

↳ If "m" is a prime, then :

↳ Factors of "m" are 1 and "m"

↳ All other positive integers are co-prime to "m"

↳ By definition of a prime, we can express Euler's Totient Function as the equation : $\phi(m) = m-1$, if "m" is a prime. Thus, "m" is prime, if and only if $\phi(m) = m-1$.

Proof # 2 : If $\phi(m) = m-1$, then "m" is prime.

↳ Fermat's Little Theorem states that if "m" is prime (and "a" is not divisible by "m"), then the equation : $a^{m-1} \equiv 1 \bmod m$ is true.

↳ By definition of Fermat's Little Theorem, "m" is prime if and only if $a^{m-1} \equiv 1 \bmod m$ evaluates as true.

Problem 5 : Compute Values of phi

a) $\phi(6)$

Solution :

Step 1 : List all prime factors of 6.

↳ 6 has prime factors $2 \cdot 3$

Step 2 : Use Euler's Phi Function for calculation

Equation: $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

↳ $\phi(6) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$

↳ $\phi(6) = 6\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)$

↳ $\phi(6) = 6\left(\frac{2}{6}\right)$

↳ $\phi(6) = 2$

$\boxed{\text{Answer : } \phi(6) = 2}$

check work : 1, ~~2~~, ~~3~~, ~~4~~, 5, ~~6~~

↳ common factors : 2, 3, 4, 6 (4 values)

↳ coprimes : 1, 5 (2 values) ✓

b) $\phi(9)$

Solution :

Step 1 : List all prime factors of 9.

↳ 9 has prime factors $3 \cdot 3$

Step 2 : Use Euler's Phi Function for calculation.

Equation : $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

↳ $\phi(9) = 9\left(1 - \frac{1}{3}\right)$

↳ $\phi(9) = 9\left(\frac{2}{3}\right)$

↳ $\phi(9) = 6$

$\boxed{\text{Answer : } \phi(9) = 6}$

---

check work : 1, 2, ~~3~~, 4, 5, ~~6~~, 7, 8, ~~9~~

↳ common factors : 3, 6, 9 (3 values)

↳ coprimes : 1, 2, 4, 5, 7, 8 (6 values) ✓

c) $\phi(15)$

Solution:

Step 1: List all prime factors of 15.

↳ 15 has prime factors $3 \cdot 5$

Step 2: Use Euler's Phi Function for calculation

Equation: $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

↳ $\phi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$

↳ $\phi(15) = 15\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$

↳ $\phi(15) = 15\left(\frac{8}{15}\right)$

↳ $\phi(15) = 8$

$$\boxed{\text{Answer: } \phi(15) = 8}$$

Check work: 1, 2, ~~3~~, 4, ~~5~~, ~~6~~, 7, 8, ~~9~~, ~~10~~, 11, ~~12~~, 13, 14, ~~15~~

↳ common factors: 3, 5, 6, 9, 10, 12, 15 (7 values)

↳ coprime: 1, 2, 4, 7, 8, 11, 13, 14 (8 values) ✓

d) $\phi(17)$

Solution :

Step 1 : List all prime factors of 17.

↳ 17 has prime factors $17 \cdot 1$

Step 2 : Use Euler's Phi Function for calculation.

Equation : $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

↳ $\phi(17) = 17\left(1 - \frac{1}{17}\right)$

↳ $\phi(17) = 17\left(\frac{16}{17}\right)$

↳ $\phi(17) = 16$

$\boxed{\text{Answer : } \phi(17) = 16}$

---

check work : 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, ~~17~~

↳ common factors : 17 (1 value)

↳ coprime : 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 (16 values) ✓

References

Student Discussions

- Chidanand Bangalore
- Satya Srinivas
- Iyioluwa Aromokudu
- Naphi Tang
- Aaron Couch
- Matthew Holmes
- Nahid Farady
- Lauren Ayala

office Hours

Tools and Resources

- Hoffstein textbook
- Async video (module 1)
- Youtube
- Wikipedia
- Stack Exchange
- Khan Academy
- Berkeley EECS Handout
- Wolfram Alpha