Cryptography - Day 11: The RSA Cipher

MA 111: Intro to Contemporary Math

October 21, 2013
Review: DHM Key Mechanics

Example
Two parties, Alice and Bob, calculate a key that a third person Carl will never know, even if Carl intercepts all communication between Alice and Bob.

First off, Alice & Bob agree on numbers $n$ and $M$ (not secret).

What Alice does:
1. Choose a secret value $a$.
2. Compute $\alpha = M^a \pmod n$.
3. Sends $\alpha$ to Bob.
4. Receives $\beta$ from Bob.
5. Key is $K = \beta^a \pmod n$.

What Bob does:
1. Choose a secret value $b$.
2. Compute $\beta = M^b \pmod n$.
3. Sends $\beta$ to Alice.
4. Receives $\alpha$ from Alice.
5. Key is $K = \alpha^b \pmod n$. 
Bob and Alice are trying to send a key over unsecured communication lines. They agree to use $M = 10$ and $n = 41$.

- Compute $M^5 \pmod{n} = 10^5 \pmod{41}$.

- Can you use your answer above to easily calculate $\alpha = M^{17} \pmod{41}$?
Bob and Alice are trying to send a key over unsecured communication lines. They agree to use $M = 10$ and $n = 41$. Alice receives $\beta = 18 \pmod{41}$ from Bob. Her secret value is $a = 13$.

- Calculate $\beta^4 \pmod{41} = 18^4 \pmod{41}$.

- Use your answer above to quickly calculate $\beta^{12} \pmod{41} = (18^4)^3 \pmod{41}$.

- What is the key for this exchange?
You’ve been promoted to the highest rank in the Spy Agency! It’s now time to learn about a modern and sophisticated code. See if you can handle the following questions:

- If $p = 41$ and $q = 53$, find $n$ and $m$.
- If $p = 101$ and $q = 107$, find $n$ and $m$.
- If $p = 521$ and $q = 641$, find $n$ and $m$. 
You’ve been promoted to the highest rank in the Spy Agency! It’s now time to learn about a modern and sophisticated code. See if you can handle the following questions:

- If \( p = 17 \) and \( q = 19 \), find \( n \) and \( m \).
- If \( p = 7 \) and \( m = 132 \), find \( q \) and \( n \).
- If \( p = 3 \) and \( q = 5 \), find all units \((\text{mod } m)\).
- If \( p = 5 \) and \( q = 11 \), what is \( 27 \cdot 3(\text{mod } m) \)?
Encryption: RSA Cipher

Definition

The RSA Cipher is a public key cipher publicly discovered in the 1970s. The RSA cipher uses a form of multiplication for encryption and is secure because factoring large numbers is (currently) very difficult to do.

- RSA stands for Rivest, Shamir, and Adleman, the people responsible for first publicizing the RSA cipher.

- The British and US governments may have known about RSA prior to the 1970s, but did not announce their discovery.

- Even though this is the basis for most modern cryptography, there is current speculation that the US government (specifically the NSA) has the ability to break this code.
Related Idea: RSA Encryption Step 1

Here is how Alice and Bob can do to share a secret from Carl:

What Alice Does

1. Alice chooses two (large) prime numbers $p$ and $q$, which she keeps secret.

2. She multiplies them to find $n = p \cdot q$. This can be done quickly because multiplication is “easy”.

3. Alice also calculates a value $m = (p - 1)(q - 1)$.

4. She selects a value $e(\text{mod } m)$ that is a unit.

Any choice of $e$ with $\gcd(e, m) = 1$ will work. The value $e$ is called the encryption exponent.
5. Next, Alice tells Bob (and anyone else) the values for $n$ and $e$. The fact that Alice can publicly state $n$ and $e$ is what makes RSA a public key cipher.

What Bob Does To Send Alice a Message

6. Bob converts letters (or blocks of letters) into numbers. We can do this is the standard way, but in real-life this gets done by a computer.

7. He uses the encryption rule $\square^e \pmod{n} = \square$ and then sends the resulting ciphertext to Alice.
A fellow agent wants you to send her a message. She broadcasts the numbers $n = 33$ and $e = 3$, expecting that these will be intercepted.

- Use this RSA cipher to encrypt the letter “H” as a number.
- Use this RSA cipher to encrypt the letter “I” as a number.
- Use this RSA cipher to encrypt the letter “J” as a number.
- The letters “H”, “I” and “J” are consecutive. Does RSA encrypt these letters as consecutive numbers?
You want a fellow agent to send you a secret message. You decide on the numbers $n = 77$ and $e = 7$ and publish these to an open webpage.

- What number will the letter “B” be encrypted as?

- What number will the letter “C” be encrypted as?

- Encrypt the number “0203”? Is this connected to the answers above in any way?
Related Idea: RSA Decryption

1. Alice knows $p$, $q$, and $m = (p - 1) \cdot (q - 1)$.

2. She can easily find the value $d$ that is the multiplicative inverse to $e \pmod{m}$. This $d$ is called the decryption exponent.

3. Alice takes the ciphertext she receives from Bob uses the decryption rule: $\text{\ding{113}}^d \pmod{n} = \square$.

This works because $e$ and $d$ are multiplicative inverses, and we have an algebra rule that says $\text{\ding{113}}^d = (\square^e)^d = \square^{e \cdot d}$. 
Homework Assignments

1. HW 9 - Cryptography 5 - due Tues 10/22 - 6:00 AM
2. HW 10 - Cryptography 6 - due Thurs 10/24 - 6:00 AM
3. Prepare for Exam 2 - Friday, 10/26