Intermediate Math Circles
April 2, 2014
Cryptography III

RSA Encryption Scheme:

RSA is a **public-key** encryption scheme published in 1977 by mathematicians Rivest, Shamir and Adleman.

Last week: How to pick the keys

Setup:

In general:	Example:
I choose distinct primes p and q. (p and q are usually very large)	$p = 11, q = 13$
Let $n = pq$ Let $m = (p-1)(q-1)$	$n = 11(13) = 143$ $m = 10(12) = 120$
Choose $1 < e < m$ such that $\gcd(e, m) = 1$	$e = 23$
Solve $ed \equiv 1 \pmod{m}$ to get d with $0 \leq d < m$.	Solve $23d \equiv 1 \pmod{120}$ $d = 47$ (Math Circle 2, Example 4)
My public key is (e, n) - publish this	$(e, n) = (23, 143)$
My private key is (d, n) - keep this a secret	$(d, n) = (47, 143)$
I can now forget p and q	

Tonight: How to Encrypt and Decrypt

More modular arithmetic

Recall:
If a, b and m are integers,

$$a \equiv b \pmod{m}, \text{ "}a \text{ is } \textbf{congruent} \text{ to } b \text{ modulo } m\text{"}$$

means that the difference $a - b$ **is a multiple of** m,
or $a - b = km$, where k is some integer.

Math Circle 1: We looked at what happens when you add/subtract.

Math Circle 2: We looked at what happens when you multiply:

In general: If $a \equiv A \pmod{m}$ and $b \equiv B \pmod{m}$, then

$$a \cdot b \equiv A \cdot B \pmod{m}$$

Today: What about powers?
What is $a^2 \pmod{m}$?

Since $a \equiv A \pmod{m}$ and $a \equiv A \pmod{m}$, then

$$a^2 = a \times a \equiv A \times A \equiv A^2 \pmod{m}$$

Since $a \equiv A \pmod{m}$ and $a^2 \equiv A^2 \pmod{m}$, then

$$a^3 = a \times a^2 \equiv A \times A^2 \equiv A^3 \pmod{m}$$

In general: If $a \equiv A \pmod{m}$, then

$$a^n \equiv A^n \pmod{m}, \quad \text{for all } n \geq 0$$

Example 1: Reduce **Example 1:** Reduce

a) $11^3 \mod 7$

$11^3 \equiv 1331 \equiv 1 \pmod 7$ since $1331 = 7 \cdot 190 + 1$

OR

$11 \equiv 4 \pmod 7$ $\quad \therefore 11^3 \equiv 4^3 \pmod 7$

$\equiv 64 \pmod 7$

$\equiv 1 \pmod 7$

b) $4^{3456} \mod 3$

$4 \equiv 1 \pmod 3$ $\quad \therefore 4^{3456} \equiv 1^{3456} \pmod 3$

$\equiv 1 \pmod 3$

c) $47^{59} \mod 6$

$47 \equiv 5 \pmod 6$

$\therefore 47^2 \equiv 25 \pmod 6$

$\equiv 1 \pmod 6$

$47^{59} \equiv (47^2)^{29} \cdot 5 \pmod 6$

$\equiv 1^{29} \cdot 5 \pmod 6$

$\equiv 5 \pmod 6$

$47 \equiv -1 \pmod 6$

$\therefore 47^{59} \equiv (-1)^{59} \pmod 6$

$\equiv -1 \pmod 6$

$\equiv 5 \pmod 6$

Example 2: Reduce $37^{23} \pmod{143}$

When calculating $a^k \mod m$, it sometimes is easier to use the
Square and Multiply Algorithm:

First, write 23 as a sum of powers of 2:
$23 = 16 + 4 + 2 + 1$ (Aside: $23 = (10111)_2$ in binary).

Notice that $37^{23} = 37^{16}37^4 37^2 37^1$
And each of these factors can be calculated by squaring the previous terms:
$37^2 \equiv (37^1)^2 \equiv 37^2 \equiv 1369 \equiv 82 \pmod{143}$
$37^4 \equiv (37^2)^2 \equiv 82^2 \equiv 6724 \equiv 3 \pmod{143}$
$37^8 \equiv (37^4)^2 \equiv 3^2 \equiv 9 \pmod{143}$
$37^{16} \equiv (37^8)^2 \equiv 9^2 \equiv 81 \pmod{143}$

Therefore,
$37^{23} \equiv 37^{16}37^4 37^2 37^1 \pmod{143}$
$\equiv 81 \cdot 3 \cdot 82 \cdot 37 \pmod{143}$
$\equiv 243 \cdot 3034 \pmod{143}$
$\equiv 100 \cdot 31 \pmod{143}$
$\equiv 3100 \pmod{143}$
$\equiv 97 \pmod{143}$

Problem Set 1:

1. What is the reminder when 8^{38} is divided by 3?
2. Determine the remainder when 16^{47} is divided by 6.
3. If today is a Wednesday, what day of the week will it be 2^{100} days from now?
4. Is $5^{21} + 8^{41}$ divisible by 7?
5. Reduce 25^{23} modulo 143.
6. Reduce 38^{47} modulo 143.

Answers to Problem Set 1:

1. 1
2. 4
3. Friday
4. Yes
5. 38
6. 25

Encryption and Decryption with RSA:

RSA is used to decrypt and encrypt numerical messages.

If we are wanting to send English text, then we assign the letters A to Z a number, say from 00 to 25.
So MATH would become 12001907.

Let's suppose we've already set up our public key $(e, n) = (23, 143)$ and private key $(d, n) = (47, 143)$ (we set these keys up last week).

To send me a message:

In general:	Example:
You want to send me the message M.	$M = 25$
To encrypt, look up my public key (e, n)	$(e, n) = (23, 143)$
Reduce M^e modulo n That is, calculate C, with $0 \leq C < n$, such that $M^e \equiv C \pmod{n}$	Reduce 25^{23} mod 143 $25^{23} \equiv 38 \pmod{143}$ (Problem Set 1, # 5)
Send ciphertext C	$C = 38$

To decode a message:

In general:	Example:
I want to decode ciphertext C.	$C = 38$
To decode, I take my secret key (d, n)	$(d, n) = (47, 143)$
and reduce C^d modulo n That is, find R, with $0 \leq R < n$, such that $C^d \equiv R \pmod{n}$	Reduce 38^{47} mod 143 $38^{47} \equiv 25 \pmod{143}$ (Problem Set 1, # 6)
$R = M$	$R = 25 = M$

Notes:

- The fact that $R = M$ in this example is not a coincidence. It can be proven that this will always be true, we just do not have all of the tools to do so tonight.
- We need $M < n$. If you wanted to send me $M = 253649$, you would break it into pieces less than n: 25 36 49 and send each separately.

Problem Set 2:

1. In last week's Math Circle, Problem Set 2, #1, we set up the RSA key pair: public key $(e, n) = (23, 143)$, private key $(d, n) = (47, 143)$
   a) Encrypt the plaintext $M = 13$ (use the public key)
   b) Decrypt the ciphertext $C = 52$ (use the private key)

2. In last week's Math Circle, Problem Set 2, #2, we set up the RSA key pair: public key $(e, n) = (19, 115)$ private key $(d, n) = (51, 115)$
   a) Encrypt the plaintext $M = 13$ (use the public key)
   b) Decrypt the ciphertext $C = 2$ (use the private key)

3. In last week's Math Circle, Problem Set 2, #3, we set up the RSA key pair: public key $(e, n) = (29, 253)$ private key $(d, n) = (129, 253)$
   a) Encrypt the plaintext $M = 4$ (use the public key)
   b) Decrypt the ciphertext $C = 146$ (use the private key)

Answers to Problem Set 2:

1. a) 52
   b) 13
2. a) 2
   b) 13
3. a) 146
   b) 4

Why is RSA secure?

In order to read encrypted messages, we need the private key (d, n).
We already know (e, n) (this key is public), so we have n.
So we need just d.
Since we have e, we need to solve $ed \equiv 1 \pmod{m}$, so we need to know m.
$m = (p-1)(q-1)$, so to determine m, we need to know p and q.
But we know n and $n = pq$, so if we can factor n, then we can determine m, find the private key (d, n), and break the code.

Can we factor n?

If n is small, then it is not too difficult to do.
Try factoring 143.
Now try to factor 1709023.

In practice, it is recommended that p and q are large enough that all known factoring algorithms are too slow to factor n.

It is believed that as long as n cannot be factored, then it is impossible to determine the private key (d, n) from the public key (e, n).

What does quantum computing have to do with all of this?

Other Notes about the RSA encryption scheme:

RSA eliminates the problem of how to securely transmit keys, but there are still other important questions to think about:

1. When we receive an encrypted message, how do we know for sure who it's from?

2. How do we know that the message has not been altered?