Intermediate Math Circles
March 26, 2014
Cryptography II

Private-Key and Public-Key Cryptography Systems

The Caesar and Substitution Ciphers we looked at last week are examples of **Private-Key Systems**.

Private-Key Systems

In a private-key system, each pair of users need to share a common key. (For example, with the Caesar cipher, Alice and Bob might share the key $k = 7$).

If Alice and Carol wanted to share a message, they would need a different key.

Advantage: Private-key systems are often very fast.

Disadvantage: Every pair of users needs to share a different private key.
With 100 users trying to send messages to one another, how many keys would we need?
Answer: $\frac{100 \times 99}{2} = \binom{100}{2} = 4950$ keys.

Another problem: how do we safely transmit the key from Alice to Bob?

Public-Key Systems

Bob creates an encryption key k_B and a decryption key l_B. He puts k_B in a public place, and keeps l_B a secret.

If Alice (or anyone else) wants to send a message M to Bob, she encrypts M into ciphertext using k_B. Bob can then decrypt the ciphertext using l_B to get back the original message M.

Analogy: Alice puts her message in a box, puts one of Bob's padlocks on the box, and sends the box to Bob. Bob then opens the box with one of his keys.

For this system to work, we need it to be impossible (or at least practically impossible) for an eavesdropper Eve to determine Bob's secret key l_B from his public key k_B.

Alice will also have her own public key k_A and secret key l_A. If Bob (or anyone else) wants to send a message to Alice, he'll use k_A to encrypt and then Alice will use l_A to decrypt.

If 100 users are trying to send messages to one another, how many keys are needed?
Answer: 200 (100 public keys and 100 secret keys).

Also, there is no longer the problem of figuring out how to securely transmit the keys.

More modular arithmetic

Last week:
If a, b and m are integers,

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

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

For example,
$51 \equiv 2 \mod 7$, since 51 and 2 differ by a multiple of 7, or $51 - 2 = 49$ is a multiple of 7.

We also looked at happens when you add/subtract.

Today: What about multiplying?

For example:
$28 \equiv 4 \pmod 8$ and $11 \equiv 3 \pmod 8$. What happens when we multiply?

$28 \times 11 = 308 \equiv 4 \pmod 8$, since $308 = 8 \times 38 + 4$
Notice: $3 \times 4 = 12 \equiv 4 \mod 8$
Is this a coincidence?

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

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

Example 1: Reduce (in two different ways)

a) $17 \times 21 \mod 6$

b) $83 \times 21 \mod 3$

c) 192×118 modulo 5

What about dividing both sides of a congruence by an integer?

- $27 \equiv 3 \pmod 8$
  Dividing out the 3's, we get $9 \equiv 1 \pmod 8$, which is true.
- $27 \equiv 3 \pmod{12}$
  Dividing out the 3's, we get $9 \equiv 1 \pmod{12}$, which is false.

You need to be careful with division!

Solving Linear Congruences

Definition:
A relation of the form $ax \equiv c \pmod{m}$, where a, c and m are integers, is called a **linear congruence** in the variable x.

We will be interested in finding all **integer solutions** x.

For example: Solve $4x \equiv 8 \pmod{10}$ for x, where x is an integer.

Let's develop a way to solve $ax \equiv c \pmod{m}$ in general:

$$\begin{aligned} ax \equiv c \pmod{m} &\iff \text{the difference} \quad ax - c \quad \text{is a multiple of} \quad m \\ &\iff ax - c = mk \quad \text{for some integer} \quad k \\ &\iff ax - c = -my \quad \text{for some integer} \quad y \\ &\iff ax + my = c \quad \text{has a solution where } x \text{ and } y \text{ are integers.} \end{aligned}$$

Back to our example:
$4x \equiv 8 \pmod{10}$ has a solution
$\iff 4x - 8$ is a multiple of 10
$\iff 4x - 8 = -10y$ for some integer y
$\iff 4x + 10y = 8$ has a solution where x and y are integers.

Since x and y must be integers, this is just a linear Diophantine Equation!

When does the linear Diophantine Equation $ax + my = c$ have a solution?

Let $d = \gcd(a, m)$.

$ax + my = c$ has a solution if and only if $d|c$ ("d divides c").

The full set of solutions is given by

$$x = x_0 + n\left(\frac{m}{d}\right), \quad y = y_0 - n\left(\frac{a}{d}\right)$$

where n is any integer and $x = x_0,\ y = y_0$ is one integer solution to the Diophantine equation.

Example 2: Solve $4x \equiv 8 \pmod{10}$.

$4x \equiv 8 \pmod{10}$ has a solution
$\iff$ $4x + 10y = 8$ has a solution where x and y are integers.
$\iff$ gcd(4,10)|8

$\gcd(4, 10) = 2|8$; therefore, there is a solution to $4x \equiv 8 \pmod{10}$.

A particular solution to $4x + 10y = 8$: $x = 7, y = -2$

Therefore, the full solution is

$$x = 7 + n\left(\frac{10}{2}\right) = 7 + 5n$$

$$y = -2 - n\left(\frac{4}{2}\right) = -2 - 2n, \quad \text{where } n \text{ is any integer}$$

Therefore, the full solution to $4x \equiv 8 \pmod{10}$ is $x = 7 + 5n$, where n is any integer.

If we wanted the solutions to $4x \equiv 8 \pmod{10}$ with $0 \leq x < 10$, they are

$$x = 2, \ x = 7$$

Example 3: Solve $10x \equiv 3 \pmod{14}$. Determine all solutions with $0 \leq x < 14$.

$10x \equiv 3 \pmod{14}$ has a solution
$\iff$ $10x + 14y = 3$ has a solution where x and y are integers.
$\iff$ $\gcd(10, 14) \mid 3$.

$\gcd(10, 14) = 2 \nmid 3$.

Therefore, there are no integer solutions to the congruence $10x \equiv 3 \pmod{14}$.

Example 4: Solve $23x \equiv 1 \pmod{120}$.
Determine all solutions with $0 \leq x < 120$.

$23x \equiv 1 \pmod{120}$ has a solution
$\iff$ $23x + 120y = 1$ has a solution where x and y are integers.
$\iff$ gcd(23,120) | 1.
gcd(23,120) $= 1|1$; therefore there is a solution to $23x + 120y = 1$.

It is not easy to find a particular solution to $23x + 120y = 1$ by inspection.
We will find one using our work on linear Diophantine in previous Math Circles.

Step 1: Calculate the gcd(23, 120) using the Euclidean Algorithm:

$$120 = 5(23) + 5 \tag{1}$$
$$23 = 4(5) + 3 \tag{2}$$
$$5 = 1(3) + 2 \tag{3}$$
$$3 = 1(2) + 1 \tag{4}$$
$$2 = 2(1) + 0 \tag{5}$$

This tells us that gcd(23, 120) = 1.

Step 2: Find one solution to $23x + 120y = 1$ working backwards in Step 1:

$$\begin{aligned}
\text{From (4):} \quad 1 &= 3 - 1(2) \\
\text{From (3):} \quad &= 3 - 1[5 - 1(3)] = 2(3) - 1(5) \\
\text{From (2):} \quad &= 2[23 - 4(5)] - 1(5) = 2(23) - 9(5) \\
\text{From (1):} \quad &= 2(23) - 9[120 - 5(23)] = 47(23) - 9(120)
\end{aligned}$$

This tells us that $23(47) + 120(-9) = 1$ and so a particular solution is
$x = 47,\ y = -9$.

Step 3: Use the solution $x = 47,\ y = -9$ to find all solutions to
$23x + 120y = 1$:
The full solution is

$$x = 47 + n\left(\frac{120}{1}\right) = 47 + 120n$$
$$y = -9 - n\left(\frac{23}{1}\right) = -9 - 23n$$

Therefore, the full solution to $23x \equiv 1 \pmod{120}$ is $x = 47 + 120n$, where n is any integer.

The only solution to $23x \equiv 1 \pmod{120}$ with $0 \leq x < 120$ is $x = 47$.

Problem Set 1:

1. $3x \equiv 5 \pmod{13}$
   a) Find all solutions to the congruence.
   Hint: You should be able to find one solution to the corresponding Diophantine equation by inspection.
   b) Find all solutions to the congruence with $0 \leq x < 13$.
2. $15x \equiv 6 \pmod{18}$
   a) Find all solutions to the congruence.
   Hint: You should be able to find one solution to the corresponding Diophantine equation by inspection.
   b) Find all solutions to the congruence with $0 \leq x < 18$.
3. $12x \equiv 27 \pmod{50}$
   a) Find all solutions to the congruence.
   b) Find all solutions to the congruence with $0 \leq x < 50$.
4. $19x \equiv 1 \pmod{88}$
   a) Find all solutions to the congruence.
   b) Find all solutions to the congruence with $0 \leq x < 88$.

Answers to Problem Set 1:

1. a) $x = 6 + 13n$, n is any integer.
   b) $x = 6$
2. a) $x = -2 + 6n$, n is any integer.
   b) $x = 4, 10, 16$
3. No solution
4. a) $x = -37 + 88n$, n is any integer.
   b) $x = 51$

RSA Encryption Scheme:

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

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 (as we did last week).
So MATH would become 12001907.

Today: How to pick the keys

Next week: How to encrypt and decrypt

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 $0 \leq d < m$. (There is a unique solution, since $\gcd(e, m) = 1$).	Solve $23d \equiv 1 \pmod{120}$ $d = 47$ (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	

Example 5: Using primes $p = 23$, $q = 37$ and $e = 29$, determine

- public key (e, n)
- private key (d, n)

Let $n = pq = 23(37) = 851$
Let $m = (p-1)(q-1) = 22(36) = 792$

Choose $1 < e < m$ such that $\gcd(e, m) = 1$: $e = 29$ (chosen for us)

Solve $29d \equiv 1 \pmod{792}$ to get d (with $0 \leq d < 792$):

This is equivalent to solving the linear Diophantine equation $29d + 792y = 1$

The Euclidean Algorithm gives,

$$792 = 27(29) + 9 \quad (1)$$
$$29 = 3(9) + 2 \quad (2)$$
$$9 = 4(2) + 1 \quad (3)$$

Working backwards,

$$\begin{aligned} \text{From (3):} \quad 1 &= 9 - 4(2) \\ \text{From (2):} \quad &= 9 - 4[29 - 3(9)] \\ &= 13(9) - 4(29) \\ \text{From (1):} \quad &= 13[792 - 27(29)] - 4(29) \\ &= 13(792) - 355(29) \end{aligned}$$

Therefore, a particular solution to $29d + 792y = 1$ is $d = -355,\ y = 13$.
The full solution is

$$d = -355 + k\left(\frac{792}{1}\right) = -355 + 792k$$

$$y = 13 - k\left(\frac{29}{1}\right) = 13 - 29k$$

Therefore, the first solution with $0 \leq d < 792$ is $d = -355 + 792 = 437$

The public key is $(e, n) = (29, 851)$

The private key is $(d, n) = (437, 851)$

Problem Set 2:

1. Determine the private key (d, n) that corresponds to the public key $(e, n) = (23, 143)$.

   Hints:
   - $143 = 11 \times 13$.
   - We solved the congruence $23x \equiv 1 \pmod{120}$ together in Example 4.

2. Determine the private key (d, n) that corresponds to the public key $(e, n) = (19, 115)$.

   Hint: In Problem Set 1, #4 we solved the congruence $19x \equiv 1 \pmod{88}$.

3. Determine the private key (d, n) that corresponds to the public key $(e, n) = (29, 253)$.

   Hint: $253 = 11 \times 23$.

Answers to Problem Set 2:

1. Private key is $(d, n) = (47, 143)$
2. Private key is $(d, n) = (51, 115)$
3. Private key is $(d, n) = (129, 253)$

Next week:

- How to encrypt and decrypt with RSA?
- Is RSA secure? If we know the public key (e, n), can we determine the private key (d, n)?