MTH314: Discrete Mathematics for Engineers

Lecture 8: Public-Key Cryptography

Dr Ewa Infeld

Ryerson University

Chinese Remainder Theorem

Think of a number x such that

$$x \equiv 5 \ (mod \ 7)$$

and

$$x \equiv 2 \ (mod \ 4)$$

.

Chinese Remainder Theorem

Think of a number x such that

$$x \equiv 5 \ (mod \ 7)$$

and

$$x \equiv 2 \ (mod \ 4)$$

You had to go all the way up to 26. Or 54. Or 82. Every 28 numbers, there's only one of those.

Chinese Remainder Theorem

Think of a number x such that

$$x \equiv 5 \ (mod \ 7)$$

and

$$x \equiv 2 \ (mod \ 4)$$

You had to go all the way up to 26. Or 54. Or 82. Every 28 numbers, there's only one of those.

These two congruence equations have a common solution

$$x \equiv 26 \ (mod \ 28)$$

Chinese Remainder Theorem

Theorem

Suppose that m, n are coprime. Then:

1. For all integers a, b the linear congruences

$$x \equiv a \ (mod \ m), \quad x \equiv b \ (mod \ n)$$

have a common solution.

2. If we have two solutions x_0 and x_1 such that:

$$x_0 \equiv a \ (mod \ m), \quad x_0 \equiv b \ (mod \ n)$$

$$x_1 \equiv a \ (mod \ m), \quad x_1 \equiv b \ (mod \ n)$$

Then:

$$x_0 \equiv x_1 \ (mod \ m \cdot n)$$

Chinese Remainder Theorem

So how do we use that to solve systems of linear congruences?

Suppose we have two congruence equations:

$x \equiv a \ (mon \ m)$ $\qquad$ $x \equiv 5 \ (mod \ 7)$

$x \equiv b \ (mon \ n)$ $\qquad$ $x \equiv 2 \ (mod \ 4)$

where $GCD(m, n) = 1$. $\qquad$ ✓ $GCD(7, 4) = 1$

Chinese Remainder Theorem

So how do we use that to solve systems of linear congruences?

Suppose we have two congruence equations:

$x \equiv a \ (mon \ m)$ $\qquad$ $x \equiv 5 \ (mod \ 7)$

$x \equiv b \ (mon \ n)$ $\qquad$ $x \equiv 2 \ (mod \ 4)$

where $GCD(m, n) = 1$. $\qquad$ ✓ $GCD(7, 4) = 1$

We can write $x = q_1 \cdot m + a$, $x = q_2 \cdot n + b$ for some $q_1, q_2 \in \mathbb{Z}$.

$x = q_1 \cdot 7 + 5 = q_2 \cdot 4 + 2$

Chinese Remainder Theorem

So how do we use that to solve systems of linear congruences?

Suppose we have two congruence equations:

$x \equiv a \ (mon \ m)$ $\qquad$ $x \equiv 5 \ (mod \ 7)$

$x \equiv b \ (mon \ n)$ $\qquad$ $x \equiv 2 \ (mod \ 4)$

where $GCD(m, n) = 1$. $\qquad$ ✓ $GCD(7, 4) = 1$

We can write $x = q_1 \cdot m + a$, $x = q_2 \cdot n + b$ for some $q_1, q_2 \in \mathbb{Z}$.

$x = q_1 \cdot 7 + 5 = q_2 \cdot 4 + 2$

We can mod both sides of this equation by either m or n. Suppose it's n.

$q_1 \cdot m + a \equiv b \ (mod \ n)$ $\qquad$ $q_1 \cdot 7 + 1 \equiv 2 \ (mod \ 4)$

$q_1 \cdot m \equiv b - a \ (mod \ n)$ $\qquad$ $q_1 \cdot 7 \equiv 1 \ (mod \ 4)$

Now we can find a possible value for q_1 with an LDE.

Chinese Remainder Theorem

So how do we use that to solve systems of linear congruences?

Suppose we have two congruence equations:

$x \equiv a \ (mon \ m)$ $\qquad$ $x \equiv 5 \ (mod \ 7)$

$x \equiv b \ (mon \ n)$ $\qquad$ $x \equiv 2 \ (mod \ 4)$

where $GCD(m, n) = 1$. $\qquad$ ✓ $GCD(7, 4) = 1$

We can write $x = q_1 \cdot m + a$, $x = q_2 \cdot n + b$ for some $q_1, q_2 \in \mathbb{Z}$.

$x = q_1 \cdot 7 + 5 = q_2 \cdot 4 + 2$

We can mod both sides of this equation by either m or n. Suppose it's n.

$q_1 \cdot m + a \equiv b \ (mod \ n)$ $\qquad$ $q_1 \cdot 7 + 1 \equiv 2 \ (mod \ 4)$

$q_1 \cdot m \equiv b - a \ (mod \ n)$ $\qquad$ $q_1 \cdot 7 \equiv 1 \ (mod \ 4)$

Now we can find a possible value for q_1 with an LDE. $q_1 = 3$ works.

Chinese Remainder Theorem

So how do we use that to solve systems of linear congruences?

Suppose we have two congruence equations:

$x \equiv a \ (mon \ m)$ $\qquad$ $x \equiv 5 \ (mod \ 7)$

$x \equiv b \ (mon \ n)$ $\qquad$ $x \equiv 2 \ (mod \ 4)$

where $GCD(m, n) = 1$. $\qquad$ ✓ $GCD(7, 4) = 1$

$q_1 \cdot m + a \equiv b \ (mod \ n)$ $\qquad$ $q_1 \cdot 7 + 1 \equiv 2 \ (mod \ 4)$

$q_1 \cdot m \equiv b - a \ (mod \ n)$ $\qquad$ $q_1 \cdot 7 \equiv 1 \ (mod \ 4)$

Now we can find a possible value for q_1 with an LDE.

$q_1 = 3$ works.

So $x = q_1 \cdot 7 + 5 = 26$ is one solution.

Chinese Remainder Theorem

So how do we use that to solve systems of linear congruences?

Suppose we have two congruence equations:

$x \equiv a \ (mon \ m)$ $\qquad$ $x \equiv 5 \ (mod \ 7)$

$x \equiv b \ (mon \ n)$ $\qquad$ $x \equiv 2 \ (mod \ 4)$

where $GCD(m, n) = 1$. $\qquad$ ✓ $GCD(7, 4) = 1$

$q_1 \cdot m + a \equiv b \ (mod \ n)$ $\qquad$ $q_1 \cdot 7 + 1 \equiv 2 \ (mod \ 4)$

$q_1 \cdot m \equiv b - a \ (mod \ n)$ $\qquad$ $q_1 \cdot 7 \equiv 1 \ (mod \ 4)$

Now we can find a possible value for q_1 with an LDE.

$q_1 = 3$ works.

The congruence class of $x = q_1 \cdot m + a$ mod $m \cdot n$ is one solution.

So $x = q_1 \cdot 7 + 5 = 26 \ (mod \ 28)$ is one solution. ✓

Chinese Remainder Theorem

So how do we use that to solve systems of linear congruences?

Suppose we have two congruence equations:

$x \equiv a \ (mon \ m)$ $\qquad$ $x \equiv 5 \ (mod \ 7)$

$x \equiv b \ (mon \ n)$ $\qquad$ $x \equiv 2 \ (mod \ 4)$

- Check that $GCD(m, n) = 1$.
- Write the equations as $q_1 \cdot m + a = q_2 \cdot n + b$. Mod both sides by either m to get an equation for q_2, or by n to get an equation q_1.
- Solve the resulting equation with an LDE.
- Once you hav one value for q, we can find a possible x and its congruence class mod $m \cdot n$ is the common solution of the system of congruences.

Exercise 1a

$$x \equiv -4 \ (mod\ 13)$$
$$x \equiv 5002 \ (mod\ 5)$$

Exercise 1a

$$x \equiv -4 \ (mod\ 13)$$
$$x \equiv 5002 \ (mod\ 5)$$

$$x \equiv 9 \ (mod\ 13)$$
$$x \equiv 2 \ (mod\ 5)$$

Exercise 1a

$x \equiv -4 \ (mod\ 13)$
$x \equiv 5002 \ (mod\ 5)$

$x \equiv 9 \ (mod\ 13)$ $\qquad\qquad$ $x = 13 \cdot q_1 + 9$
$x \equiv 2 \ (mod\ 5)$ $\qquad\qquad$ $x = 5 \cdot q_2 + 2$

$$13 \cdot q_1 + 9 = 5 \cdot q_2 + 2$$

Mod both sides by 5:

$$13 \cdot q_1 + 4 \equiv 2 \ (mod\ 5)$$

Exercise 1a

$x \equiv -4 \ (mod\ 13)$
$x \equiv 5002 \ (mod\ 5)$

$x \equiv 9 \ (mod\ 13)$ $\qquad$ $x = 13 \cdot q_1 + 9$
$x \equiv 2 \ (mod\ 5)$ $\qquad$ $x = 5 \cdot q_2 + 2$

$$13 \cdot q_1 + 9 = 5 \cdot q_2 + 2$$

Mod both sides by 5:

$$13 \cdot q_1 + 4 \equiv 2 \ (mod\ 5)$$

$$13 \cdot q_1 \equiv 3 \ (mod\ 5)$$

Exercise 1a

$x = 13 \cdot q_1 + 9$
$x = 5 \cdot q_2 + 2$

$$13 \cdot q_1 + 9 = 5 \cdot q_2 + 2$$

Mod both sides by 5:

$$13 \cdot q_1 + 4 \equiv 2 \ (mod\ 5)$$

$$13 \cdot q_1 \equiv 3 \ (mod\ 5)$$

You should solve to LDE... except this time we can see that $q_1 = 1$ works. So $13 \cdot 1 + 9 = 22$ works. The solution is:

$$x \equiv 22 \ (mod\ 13 \cdot 5)$$

Exercise 1c

$4x \equiv 2 \ (mod\ 6)$
$3x \equiv 5 \ (mod\ 8)$

We have to solve the linear congruences first (see last lecture).

Exercise 1c

$4x \equiv 2 \ (mod\ 6)$
$3x \equiv 5 \ (mod\ 8)$

We can to solve the linear congruences first (see last lecture).

$4x \equiv 2 \ (mod\ 6)$ is equivalent to $x \equiv 2 \ (mod\ 3)$

Or we can just write the equations as:
$4x = 6 \cdot q_1 + 2$
$3x = 8 \cdot q_2 + 5$

Exercise 1c

$4x \equiv 2 \ (mod\ 6)$
$3x \equiv 5 \ (mod\ 8)$

We can to solve the linear congruences first (see last lecture).

$4x \equiv 2 \ (mod\ 6)$ is equivalent to $x \equiv 2 \ (mod\ 3)$

Or we can just write the equations as:
$x = 3 \cdot q_1 + 2$
$3x = 8 \cdot q_2 + 5$
So:

$$3(3 \cdot q_1 + 2) = 8 \cdot q_2 + 5$$

Exercise 1c

$4x \equiv 2 \ (mod\ 6)$
$3x \equiv 5 \ (mod\ 8)$

We can to solve the linear congruences first (see last lecture).

$4x \equiv 2 \ (mod\ 6)$ is equivalent to $x \equiv 2 \ (mod\ 3)$

Or we can just write the equations as:
$x = 3 \cdot q_1 + 2$
$3x = 8 \cdot q_2 + 5$
So:

$$3(3 \cdot q_1 + 2) = 8 \cdot q_2 + 5$$

Mod both sides by 8:

$$9 \cdot q_1 \equiv 7 \ (mod\ 8)$$

$q_1 = 7$ works, and gives $x = 23$. The solution is $x \equiv 23 \ (mod\ 24)$.

Fermat's Little Theorem

Theorem

If p is prime and a, p are coprime, then:

$$a^{p-1} \equiv 1 \ (mod \ p).$$

Fermat's Little Theorem

Theorem

If p is prime and a, p are coprime, then:

$$a^{p-1} \equiv 1 \ (mod \ p).$$

Example: If $p = 7$, then for any integer a that is not a multiple of 7:

$$a^6 \equiv 1 \ (mod \ 7).$$

Fermat's Little Theorem

Theorem

If p is prime and a, p are coprime, then:

$$a^{p-1} \equiv 1 \ (mod \ p).$$

Example: If $p = 7$, then for any integer a that is not a multiple of 7:

$$a^6 \equiv 1 \ (mod \ 7).$$

Example: What is the congruence class of $n^{154} \ (mod \ 23)$?

Fermat's Little Theorem

Theorem

If p is prime and a, p are coprime, then:

$$a^{p-1} \equiv 1 \ (mod \ p).$$

Example: If $p = 7$, then for any integer a that is not a multiple of 7:

$$a^6 \equiv 1 \ (mod \ 7).$$

Example: What is the congruence class of $n^{154} \ (mod \ 23)$?

$$154 = 11 \cdot 2 \cdot 7 = 22 \cdot 7$$

Fermat's Little Theorem

Theorem

If p is prime and a, p are coprime, then:

$$a^{p-1} \equiv 1 \ (mod \ p).$$

Example: If $p = 7$, then for any integer a that is not a multiple of 7:

$$a^6 \equiv 1 \ (mod \ 7).$$

Example: What is the congruence class of $n^{154} \ (mod \ 23)$?

$$154 = 11 \cdot 2 \cdot 7 = 22 \cdot 7$$

$$n^{154} = (n^{22})^7 \equiv 1^7 \equiv 1 \ (mod \ 23)$$

Fermat's Little Theorem

Theorem

If p is prime and a, p are coprime, then:

$$a^{k(p-1)} \equiv 1 \ (mod \ p),$$

for any integer k.

Diffie-Hellman Public Key Exchange

How do you send someone an encrypted message?

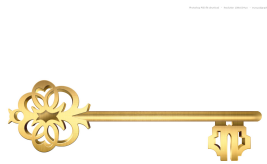
Diffie-Hellman Public Key Exchange

How do you send someone an encrypted message, if you've never met them before?

Diffie-Hellman Public Key Exchange

How do you send someone an encrypted message, if you've never met them before?

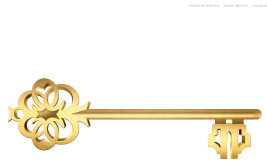
Suppose that Alice knows Bob wants to mail her something no one on the way should be able to see, but they are unable to meet in a secure location first to discuss ways to do this. One thing Alice could do would be to buy a padlock and mail an open padlock to Bob. She keeps the key. Then Bob puts the secret parcel in the box, locks it with the padlock and sends it to Alice. Alice opens it with the key.



Diffie-Hellman Public Key Exchange

How do you send someone an encrypted message, if you've never met them before?

Suppose that Alice knows Bob wants to mail her something no one on the way should be able to see, but they are unable to meet in a secure location first to discuss ways to do this. One thing Alice could do would be to buy a padlock and mail an open padlock to Bob. She keeps the key. Then Bob puts the secret parcel in the box, locks it with the padlock and sends it to Alice. Alice opens it with the key.



Two different parts: padlock (public) and key (secret, Alice keeps that.)

Diffie-Hellman Public Key Exchange

How do you send someone an encrypted message, if you've never met them before?

Suppose that Alice knows Bob wants to mail her something no one on the way should be able to see, but they are unable to meet in a secure location first to discuss ways to do this. One thing Alice could do would be to buy a padlock and mail an open padlock to Bob. She keeps the key. Then Bob puts the secret parcel in the box, locks it with the padlock and sends it to Alice. Alice opens it with the key.

Problem: what if someone intercepts Alice's padlock, switches it for their own, and sends that to Bob? Then they can intercept the parcel, look incide, lock it with Alice's padlock and send it to Alice. Alice and Bob would never know.

Diffie-Hellman Public Key Exchange

How do you send someone an encrypted message, if you've never met them before?

Suppose that Alice knows Bob wants to mail her something no one on the way should be able to see, but they are unable to meet in a secure location first to discuss ways to do this. One thing Alice could do would be to buy a padlock and mail an open padlock to Bob. She keeps the key. Then Bob puts the secret parcel in the box, locks it with the padlock and sends it to Alice. Alice opens it with the key.

Problem: what if someone intercepts Alice's padlock, switches it for their own, and sends that to Bob? Then they can intercept the parcel, look incide, lock it with Alice's padlock and send it to Alice. Alice and Bob would never know. This is a "man in the middle" attack (MITM). We'll come back to it later.

Diffie-Hellman Public Key Exchange

When we're sending information between computers, we need to do all of that with math.

Alice needs a piece of math that she can publish (say, on her webpage) that anyone can download and use to encrypt a message. She keeps another piece of math secret, that decrypts that particular public piece of math.

Diffie-Hellman Public Key Exchange

When we're sending information between computers, we need to do all of that with math.

Alice needs a piece of math that she can publish (say, on her webpage) that anyone can download and use to encrypt a message. She keeps another piece of math secret, that decrypts that particular public piece of math.

We need an encryption process that an evesdropper can't reverse even if they know the public key. We need a *trapdoor function.*

Diffie-Hellman Public Key Exchange

When we're sending information between computers, we need to do all of that with math.

Alice needs a piece of math that she can publish (say, on her webpage) that anyone can download and use to encrypt a message. She keeps another piece of math secret, that decrypts that particular public piece of math.

We need an encryption process that an evesdropper can't reverse even if they know the public key. We need a *trapdoor function.*

TRAPDOOR FUNCTIONS ARE FUNCTIONS

THAT COMPUTERS CAN DO EASILY

BUT CAN'T EASILY REVERSE

Diffie-Hellman Public Key Exchange

When we're sending information between computers, we need to do all of that with math.

Alice needs a piece of math that she can publish (say, on her webpage) that anyone can download and use to encrypt a message. She keeps another piece of math secret, that decrypts that particular public piece of math.

We need an encryption process that an evesdropper can't reverse even if they know the public key. We need a *trapdoor function.*

TRAPDOOR FUNCTIONS ARE FUNCTIONS

THAT COMPUTERS CAN DO EASILY

BUT CAN'T EASILY REVERSE

For a computer multiplication is easy, but factoring is hard.

Example: Modular Ciphers

We're going to use this form of Fermat's Little Theorem:

Theorem

If p is prime and a, p are coprime, and k is an integer then:

$$a^{k(p-1)+1} \equiv a \ (mod \ p).$$

Example: Modular Ciphers

We're going to use this form of Fermat's Little Theorem:

Theorem

If p is prime and a, p are coprime, and k is an integer then:

$$a^{k(p-1)+1} \equiv a \ (mod \ p).$$

If you have $k(p-1)+1 = e \cdot d$ for some intigers e, d, you can publish (p, e) (that's your open padlock.) If someone wants to send you a message $0 < m < p$ they actually send $c = m^e \ (mod \ p)$.

You take that encrypted message $c = m^e$ and decrypt it with d (that's the key you keep secret.)

$$c^d \ (mod \ p) \equiv (m^e)^d \equiv m^{e \cdot d} \equiv m$$

Example: Modular Ciphers

We're going to use this form of Fermat's Little Theorem:

Theorem

If p is prime and a, p are coprime, and k is an integer then:

$$a^{k(p-1)+1} \equiv a \ (mod \ p).$$

If you have $k(p-1)+1 = e \cdot d$ for some intigers e, d, you can publish (p, e) (that's your open padlock.) If someone wants to send you a message $0 < m < p$ they actually send $c = m^e \ (mod \ p)$.

Taking m to power $e \cdot d$ and then evaluating the congruence mod p is taking it full circle. Bob can take it part of the way with $m^e \ (mod \ p)$. But Alice is the only one who knows how far more exactly makes full circle, i.e. the number d.

Example: Modular Ciphers

Theorem

If p is prime and a, p are coprime, and k is an integer then:

$$a^{k(p-1)+1} \equiv a \ (mod \ p).$$

In other words, let's find $k(p-1)+1$ that splits up into two factors $k(p-1)+1 = e \cdot d$. We will use the number e for encryption, and the number d for decryption.

The pair (p, e) is your public key. You keep the secret key d.

If someone wants to send you a message m they encrypt it as $c = m^e \ (mod \ p)$ and send that instead. c stands for *ciphertext.* You need d to decrypt it.

$$(m^e)^d \equiv m \ (mod \ p)$$

RSA

Now Alice needs to generate:

- Two big primes p, q. Then calculate $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$.
- Numbers e, d such that $e \cdot d \equiv 1 \ (mod \ \phi(n))$

Alice's public key is (n, e). Her secret key is d.

RSA

Now Alice needs to generate:

- Two big primes p, q. Then calculate $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$.
- Numbers e, d such that $e \cdot d \equiv 1 \ (mod \ \phi(n))$

Alice's public key is (n, e). Her secret key is d.

Why is $\phi(n)$ well defined?

RSA

Now Alice needs to generate:

- Two big primes p, q. Then calculate $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$.
- Numbers e, d such that $e \cdot d \equiv 1 \ (mod \ \phi(n))$

Alice's public key is (n, e). Her secret key is d.

Why is $\phi(n)$ well defined?
Unique prime factorization. Think about it!

RSA

Now Alice needs to generate:

- Two big primes p, q. Then calculate $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$.
- Numbers e, d such that $e \cdot d \equiv 1 \ (mod \ \phi(n))$

Alice's public key is (n, e). Her secret key is d.

Bob sends Alice a message m in an encrypted form

$$c = m^e \ (mod \ n).$$

RSA

Now Alice needs to generate:

- Two big primes p, q. Then calculate $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$.
- Numbers e, d such that $e \cdot d \equiv 1 \ (mod \ \phi(n))$

Alice's public key is (n, e). Her secret key is d.

Bob sends Alice a message m in an encrypted form

$$c = m^e \ (mod \ n).$$

Notice that since $e \cdot d \equiv 1 \ (mod \ (p-1)(q-1))$, then we know for sure that $e \cdot d \equiv 1 \ (mod \ p-1)$. $e \cdot d = q(p-1)(q-1) + 1$

RSA

Now Alice needs to generate:

- Two big primes p, q. Then calculate $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$.
- Numbers e, d such that $e \cdot d \equiv 1 \ (mod \ \phi(n))$

Alice's public key is (n, e). Her secret key is d.

Bob sends Alice a message m in an encrypted form

$$c = m^e \ (mod \ n).$$

Notice that since $e \cdot d \equiv 1 \ (mod \ (p-1)(q-1))$, then we know for sure that $e \cdot d \equiv 1 \ (mod \ p-1)$. $e \cdot d = q(p-1)(q-1) + 1$

So $m^{e \cdot d} \equiv m \ (mod \ p)$ by FLT. Alice has $m^e \ (mod \ n)$.

RSA

Now Alice needs to generate:

- Two big primes p, q. Then calculate $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$.
- Numbers e, d such that $e \cdot d \equiv 1 \ (mod \ \phi(n))$

Alice's public key is (n, e). Her secret key is d.

Notice that since $e \cdot d \equiv 1 \ (mod \ (p-1)(q-1))$, then we know for sure that $e \cdot d \equiv 1 \ (mod \ p-1)$. $e \cdot d = q(p-1)(q-1)+1$
Similarly, $e \cdot d \equiv 1 \ (mod \ q-1)$

So $m^{e \cdot d} \equiv m \ (mod \ p)$ and $m^{e \cdot d} \equiv m \ (mod \ p)$ by FLT. Alice recieved $m^e \ (mod \ n)$ from Bob. We need to show that $m^{e \cdot d} \equiv m \ (mod \ n)$.

Let $x = c^d$, and:
$x \equiv m \ (mod \ p)$,
$x \equiv m \ (mod \ q)$.
We want to show that $x \equiv m \ (mod \ p \cdot q)$.

By the Chinese Remainder Theorem, only one number between 1 and n han satisfy both $x \equiv m \ (mod \ p)$, $x \equiv m \ (mod \ q)$. So this number has to be m itself.

We conclude that:

$$c^d \equiv m \ (mod \ n),$$

so Alice decrypted the message correctly.

RSA Example

Pick some primes p, q and find e, d such that $e \cdot d \equiv 1 \ (mod \ (p-1)(q-1))$.

What are your public and secret keys?

RSA Example

Pick some primes p, q and find e, d such that $e \cdot d \equiv 1 \ (mod \ (p-1)(q-1))$.

What are your public and secret keys?

Let's try $p = 11, \ q = 7$. Then $n = 77$ and $\phi(n) = 60$. We can pick $e = 11$, $d = 11$, then $e \cdot d = 121 \equiv 1 \ (mod \ 60)$.

RSA Example

Pick some primes p, q and find e, d such that $e \cdot d \equiv 1 \ (mod \ (p-1)(q-1))$.

What are your public and secret keys?

Let's try $p = 11, \ q = 7$. Then $n = 77$ and $\phi(n) = 60$. We can pick $e = 11$, $d = 11$, then $e \cdot d = 121 \equiv 1 \ (mod \ 60)$.

The public key is $(n, e) = (77, 11)$
The secret key is $d = 11$

RSA Example

Pick some primes p, q and find e, d such that $e \cdot d \equiv 1 \ (mod \ (p-1)(q-1))$.

What are your public and secret keys?

Let's try $p = 11, \ q = 7$. Then $n = 77$ and $\phi(n) = 60$. We can pick $e = 11$, $d = 11$, then $e \cdot d = 121 \equiv 1 \ (mod \ 60)$.

The public key is $(n, e) = (77, 11)$
The secret key is $d = 11$

An encrypted message looks like:

$$c = m^e \ (mod \ n) = m^{11} \ (mod \ 77)$$

Which is then decrypted using:

$$c^{11} \equiv m \ (mod \ 77)$$

Cryptographic signatures

So let's go back to the problem of the *man in the middle attack.*

To make sure that he has the right public key, Bob can check its *fingerprint* that Alice can post somewhere independently. Alternatively, if Alice has Bob's public key, Bob can *sign* the message.

Notice that e, d are completely symmetric in these calculations. The key opens the padlock, but in the math version the padlock also opens the key.

Bob can use his *secret* key to encrypt something, and then Alice uses Bob's *public* key to decrypt it. If this works, that means only Bob could have sent it because only he has the secret key!

Cryptographic signatures, version I

Bob can use his *secret* key to encrypt something, and then Alice uses Bob's *public* key to decrypt it. If this works, that means only Bob could have sent it because only he has the secret key!

Alice's public key is (p, e). Alice's secret key is d.
Bob's public key is (p', e'). Bob's secret key is d'.

A *signed and encrypted message* $m < p, p'$ from Bob to Alice looks like this:

$$c = ((m)^e \ (mod \ p))^{d'} \ (mod \ p')$$

Alice can decrypt it in two stages. First with Bob's *public* key:

$$c^{e'} \equiv [(m)^e \ (mod \ p)] \ (mod \ p')$$

Then with her own secret key:

$$(c^{e'})^d \equiv m \ (mod \ p)$$

Cryptographic signatures, version II

Bob can use his *secret* key to encrypt something, and then Alice uses Bob's *public* key to decrypt it. If this works, that means only Bob could have sent it because only he has the secret key!

Alice's public key is (p, e). Alice's secret key is d.
Bob's public key is (p', e'). Bob's secret key is d'.

In reality, Bob may want Alice to read his message even if she doesn't have his public key. In that case he may want to encrypt a separate token m' with his secret key, and be able to additionally verify its origin if she does. The message from Bob to Alice will be a pair (m,m') $m, m' < p, p'$, Bob sends it in the following form:

$$(c, c') = ((m)^e \pmod{p}, (m')^{d'} \pmod{p'})$$

Then Alice can independently read the message m (using her secret key) and verify the tokem m' (using Bob's public key.)