Discrete Mathematics, Section 001, Fall 2016

Lecture 21: Public key cryptography

Zsolt Pajor-Gyulai
zsolt@cims.nyu.edu

Courant Institute of Mathematical Sciences

December 5, 2016

Outline

The setting

In the schoolyard, Alice secretly wants to tell Bob that she likes him. Unfortunately, gossip girl Eve is listening. Can Alice tell Bob the secret?

- They could create a secret code, and talk in that code but Eve would hear the code then!
- They could make up the code privately, but that is impractical, it's hard to get privacy on the schoolyard.
- Fortunately, Bob is a math prodigy knows another way.

Key: Find a procedure that is easy to do but it is extremely hard to undo.

Factoring primes

- If you have primes p and q computing $n = pq$ is extremely easy.
- However, if you are given n and the knowledge that it is a product of primes, finding these prime factors is extremely hard.

Conjecture

There is no computationally efficient procedure for factoring positive integers.

Think

$$p, q \text{ are 500 digit numbers} \quad \rightarrow \quad n \text{ is a 1000 digit number}$$

In this case our best algorithms and computers would take about a century.

Procedure

1. Alice wants to say 'I like you', but she can only tell Bob a big number. So first, she encodes this using ASCII:

I		I	i	k	e		y	o	u
073	032	108	105	107	101	032	121	111	117

So Alice's number is:

$$M = 73032108105107101032121111117$$

2. Bob, in his mind creates a pair of functions E and D that are inverses of one another:

$$D(E(M)) = M$$

Procedure

1. Alice wants to say 'I like you', but she can only tell Bob a big number. So first, she encodes this using ASCII:

$$M = 73032108105107101032121111117$$

2. Bob, in his mind create a pair of functions E and D that are inverses of one another:

$$D(E(M)) = M$$

3. Bob tells Alice the function E. Eve overhears this but she's bad at math so she has no idea how to invert E to get D.
4. Using Bob's encryption function E, Alice computes $N = E(M)$ and tells N to Bob. Eve overhears this, but since she doesn't know what D is, she can't extract M.
5. Bob now uses his decryption function D in his mind to get

$$M = D(N) = D(E(M)).$$

1. In private, Bob creates a public encryption function E and a secret decryption function D.
2. Bob sends his public encryption function E to Alice. (E ←)
3. In private, Alice writes her message in ASCII, M. She uses Bob's function E to calculate $N = E(M)$.
4. Alice sends N to Bob. (N →)
5. In private, Bob uses his decryption function D to calculate $M = D(N)$. He now has Alice's message.

Eve sees E and N, but cannot calculate M from these.

Outline

The encryption function

Let n be a large integer. Set the encryption function to be

$$E(M) = M^2 \bmod n$$

What should n be?

- If Alice wants to send a message with c characters, then M will have $3c$ digits (up to the initial zeroes) and M^2 will have $6c$ digits.
- If the digits of n is more than $6c$ then $M^2 \bmod n = M^2$ and Eve can get to the message by computing the ordinary square root.
- You don't want to loose information so the number of digits of n should be at least $3c$.

$$\#\text{digits}(M) < \#\text{digits}(n) < 2 \cdot \#\text{digits}(M)$$

The encryption function

In our example,

$$M = 730321081051071010321211111117$$

which has 29 digits. So if Bob expects such a large message, he can look up two big primes

$$p = 977555333111111, \qquad q = 988666444111111$$

and multiply them to get

$$n = 966476155599814608692148154321$$

which will do. This is what Bob sends Alice who then encrypts

$$N = E(M) = M^2 \bmod n = 412976518048000543454453602839$$

which she sends back to Bob.

The encryption function

In our example,

$$M = 730321081051071010321211111117$$

$$p = 977555333111111, \qquad q = 988666444111111$$

$$n = 966476155599814608692148154321$$

$$N = E(M) = M^2 \bmod n = 412976518048000543454453602839$$

- Eve now has both n and N but she doesn't have p and q. Therefore she cannot invert E to find D and can't extract M.
- Bob knows p and q and N and as we will see, he can invert easily.

Square roots in $\mathbb{Z}_n$

$$E(M) = M^2 \bmod n$$

If Bob gets $N \in \mathbb{Z}_n$, then to find $M = D(N)$, he needs to take a square root in $\mathbb{Z}_n$.

In other words, we need to solve $x \otimes x = N$.

For example, by simple brute force

- In $\mathbb{Z}_{59}$, we have $\sqrt{17} = 28, 31$.
- In $\mathbb{Z}_{59}$, we have no $\sqrt{18}$.
- In $\mathbb{Z}_{1121}$, we have $\sqrt{17} = 146, 500, 621, 975$.
- Of course, for huge n, this is ridiculous.

Quadratic residues

$$E(M) = M^2 \bmod n$$

The encrypted message will be a 'perfect square' in $\mathbb{Z}_n$.

Definition

Let n be a positive integer and let $a \in \mathbb{Z}_n$. If there is an element $b \in \mathbb{Z}_n$ such that $a = b \otimes b$, we call a a **quadratic residue modulo** n. Otherwise we call a a quadratic nonresidue.

Motivation behind the name:

$$b \otimes b = b^2 \bmod n$$

So N is a quadratic residue modulo n.

Square roots when n is a prime

Things are relatively simple when n is a prime.

Proposition

Let p be a prime and let $a \in \mathbb{Z}_p$. Then a has at most two square roots in $\mathbb{Z}_p$.

FTSC suppose that a has three (or more) square roots in $\mathbb{Z}_p$.

Note that if x is a square root of a,

$$(-x) \otimes (-x) = (-x)^2 \bmod p = x^2 \bmod p = x \otimes x = a.$$

and therefore $-x = 0 \ominus x$ (in $\mathbb{Z}_p$) is also a square root.

Since a has three or more roots, we can choose two of them $x, y \in \mathbb{Z}_p$, such that $x \neq \pm y$. Then

$$(x - y)(x + y) \bmod p = x^2 - y^2 \bmod p = x^2 \ominus y^2 = a - a = 0$$

[...]

Proposition

Let p be a prime and let $a \in \mathbb{Z}_p$. Then a has at most two square roots in $\mathbb{Z}_p$.

[...]

Since a has three or more roots, we can choose two of them $x, y \in \mathbb{Z}_p$, such that $x \neq \pm y$. Then

$$(x - y)(x + y) \bmod p = x^2 - y^2 \bmod p = x^2 \ominus y^2 = a - a = 0$$

But this means that $p|(x - y)(x + y)$, which implies (as p is prime) that

$$p|(x - y) \qquad \text{or} \qquad p|(x + y)$$

However, since $x \neq \pm y$ and $0 \leq x, y < p$, this is not possible. $\Rightarrow\Leftarrow$. □

An auxiliary result

Fermat's little theorem

Let p be a prime and let a be an integer. Then

$$a^p \equiv a \pmod{p}$$

For example, $5^{23} \equiv 5 \pmod{23}$.

This has a generalization:

Euler's theorem

Let n be a positive integer and let a be an integer relatively prime to n. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

For proofs, see the textbook.

Identification of quadratic residues in $\mathbb{Z}_p$ for special p.

Proposition

Let p be a prime of the form $p = 4k + 3$ for some $k \in \mathbb{N}$. Let $a \in \mathbb{Z}_p$ be a quadratic residue. Then the square roots of a in $\mathbb{Z}_p$ are

$$\left[\pm a^{\frac{p+1}{4}}\right] \mod p.$$

By the restriction on p, $\frac{p+1}{4}$ is an integer and everything makes sense. Since a is a quadratic residue, there is an $x \in \mathbb{Z}_p$ such that $x^2 \equiv a \pmod{p}$. Then

$$\left[\pm a^{\frac{p+1}{4}}\right]^2 \equiv \left[x^{\frac{p+1}{2}}\right]^2 = x^{p+1} = x^p x \equiv x^2 \equiv a \pmod{p}.$$

where Fermat's little theorem was used. By the previous Proposition, there are no more roots. □

$n = pq$ where p and q are primes of the form $4k + 3$.

We still want to solve $x \otimes x = N$ in $\mathbb{Z}_n$. This is the same as

$$x^2 \bmod n = N$$

which means that for some $k \in \mathbb{Z}$,

$$x^2 = kn + N = k(pq) + N$$

But this means both

$$x^2 = (kp)q + N, \qquad x^2 = (kq)p + N$$

or

$$x^2 \bmod p = N \qquad x^2 \bmod q = N.$$

But if x_1 is a square root of N in $\mathbb{Z}_p$ and x_2 is a square root of N in $\mathbb{Z}_q$ (which we now know how to compute for our special primes), then an x satisfying both

$$x = x_1 + k_1 q \qquad x = x_2 + k_2 p$$

for some $k_1, k_2 \in \mathbb{Z}$ does the job.

In our example

For Bob's public key

$$n = 966476155599814608692148154321$$

he has that

$$p = 977555333311111, \qquad q = 988666444411111$$

are both of the form $4k + 3$ and therefore

- $\sqrt{N}$ in $\mathbb{Z}_p$ is

  $$\pm N^{\frac{p+1}{4}} \bmod p = \pm N^{244388833327778} \bmod p = \pm 869000357225117$$

- $\sqrt{N}$ in $\mathbb{Z}_q$ is

  $$\pm N^{\frac{q+1}{4}} \bmod q = \pm N^{988666444411111} \bmod q = \pm 154623490704086$$

In other words

$$x_1 = 869000357225117, 108554976085994$$

$$x_2 = 154623490704086, 834042953707025$$

Chinese remainder theorem

$$x_1 = 869000357225117, 108554976085994$$

$$x_2 = 154623490704086, 834042953707025$$

This gives four equation of the form

$$x = x_1 + k_1 p \qquad x = x_2 + k_2 q$$

or in other words

$$x \equiv x_1 \pmod{p}, \qquad x \equiv x_2 \pmod{q}$$

Chinese remainder theorem

The pair of congruences

$$x \equiv x_1 \pmod{p}, \qquad x \equiv x_2 \pmod{q}$$

has a unique solution x_0 with $0 \leq x_0 < pq$. Furthermore, every mutual solution to these congruences differs from x_0 by a multiple of mn.

In our example

We earlier got

$$x_1 = 869000357225117, 108554976085994$$

$$x_2 = 154623490704086, 834042953707025$$

If p^{-1} is the reciprocal of p in $\mathbb{Z}_q$,

$$M = x_0 = x_1 + \left[((x_2 - x_1) \bmod q) \otimes p^{-1}\right] p \bmod n$$

Two independent possibilites for x_1 and x_2 gives us four x_0-s. The Euclidean algorithm yields

$$-174529541694500p + 172568094394491q = 1$$

and thus in $\mathbb{Z}_q$,

$$p^{-1} = -174529541694500 \bmod q = 814136902716611$$

In our example

We earlier got

$$x_1 = 869000357225117, 108554976085994$$

$$x_2 = 154623490704086, 834042953707025$$

For each pair x_1, x_2,

$$M = x_1 + \left[((x_2 - x_1) \bmod q) \otimes p^{-1}\right] p \bmod n$$

$$p^{-1} = 814136902716611$$

This gives the following four M values:

$$M_1 = 730321081051071010321211111117$$

$$M_2 = 811685135902651145620250169817$$

$$M_3 = 893444047494707507660027043204$$

$$M_4 = 154791019697163463071897984504$$

In our example

This gives the following four M values:

$$M_1 = 730321081051071010321211111117$$

$$M_2 = 811685135902651145620250169817$$

$$M_3 = 893444047494707507660027043204$$

$$M_4 = 154791019697163463071897984504$$

To see if any of this is the actual message, do inverse ASCII:

$M_1 \rightarrow$ I like you $\quad M_2 \rightarrow Junk \quad M_3 \rightarrow Junk \quad M_4 \rightarrow Junk$

So the message is clearly discernable for Bob.

Summary

After Bob gets N,

- Compute $\sqrt{N}$ in $\mathbb{Z}_p$ and $\mathbb{Z}_q$.
- This gives four pairs for (x_1, x_2).
- For each pair solve the Chinese remainder problem and get an M.
- Out of the four M-s, three will be gibberish, the remaining one is the original M.

Outline

Euler's totient

Definition

For every positive integer n, let $\varphi(n)$ denote the number of integers from 1 to n inclusive that are relatively prime to n.

For example,

- For $n = 14$, $\{1, 3, 5, 9, 11, 13\}$ are the relative primes to n and therefore $\varphi(14) = 6$.
- For $n = 15$, $\{1, 2, 4, 7, 8, 11, 13, 14\}$ are the relative primes to n and therefore $\varphi(15) = 8$.

Theorem

If the prime factorization of n is $p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}$, then

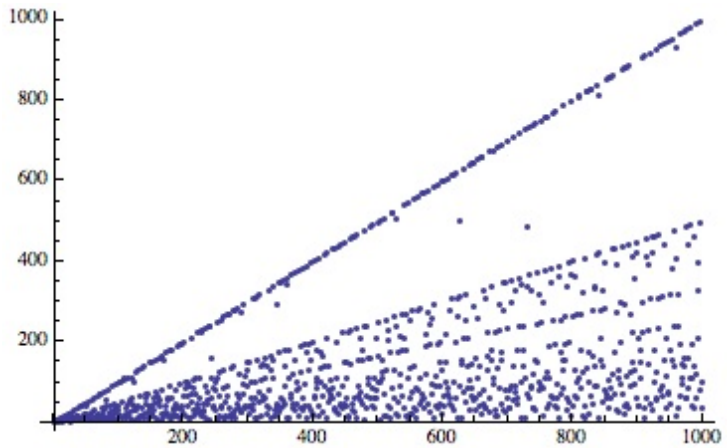
$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_t}\right)$$

Euler's totient

Theorem

If the prime factorization of n is $p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}$, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_t}\right)$$



An auxiliary result

Fermat's little theorem

Let p be a prime and let a be an integer. Then

$$a^p \equiv a \pmod{p}$$

For example, $5^{23} \equiv 5 \pmod{23}$.

This has a generalization:

Euler's theorem

Let n be a positive integer and let a be an integer relatively prime to n. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

For proofs, see the textbook.

The encryption function

$$E(M) = M^e \bmod n, \qquad D(N) = N^d \bmod n$$

for appropriately chosen e and d and $n = pq$ as before.

$$D(E(M)) = D(M^e \bmod n) = M^{ed} \bmod n$$

By Euler's theorem, we know that

$$M^{\varphi(n)} = 1 \qquad \text{in } \mathbb{Z}_n$$

and therefore

$$M^{k\varphi(n)+1} = (M^{\varphi(n)})^k M = 1^k M = M \qquad \text{in } \mathbb{Z}_n$$

and so we want $ed = k\varphi(n) + 1$.

The encryption function

$$E(M) = M^e \bmod n, \qquad D(N) = N^d \bmod n$$

We want $ed = k\varphi(n) + 1$.

- Since Bob knows p and q, he can compute $\varphi(n)$ easily.
- Bob selects his favorite $e \in \mathbb{Z}_{\varphi(n)}$.
- Then he computes $d = e^{-1} \in \mathbb{Z}_{\varphi(n)}$.
- He tells Alice n and e publicly (so that Eve can hear), but keeps p, q and d a secret.
- Alice computes $N = E(M)$ using Bob's key and sends N to Bob.
- Eve knows n, e, but he cannot find $D(N)$ as he can't find $\varphi(n)$.
- Bob decodes $M = D(N)$ and they live happily ever after.