Aspects of Elliptic Curve Cryptography

21C3

27. December 2004

Florian Heß
Technische Universität Berlin

www.math.tu-berlin.de/∼hess

Overview

Reminder of basic cryptographic tasks

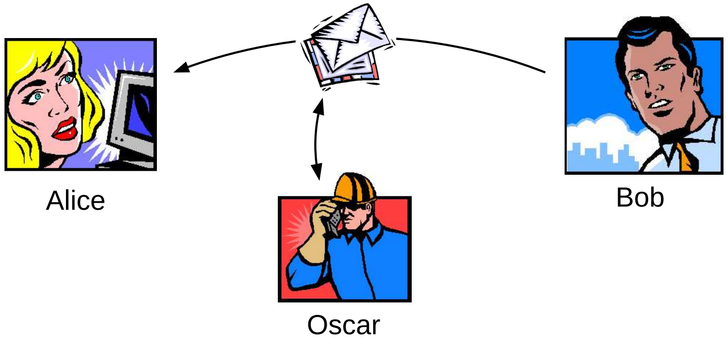
Finite fields, ElGamal encryption

Group based cryptography

Elliptic curves

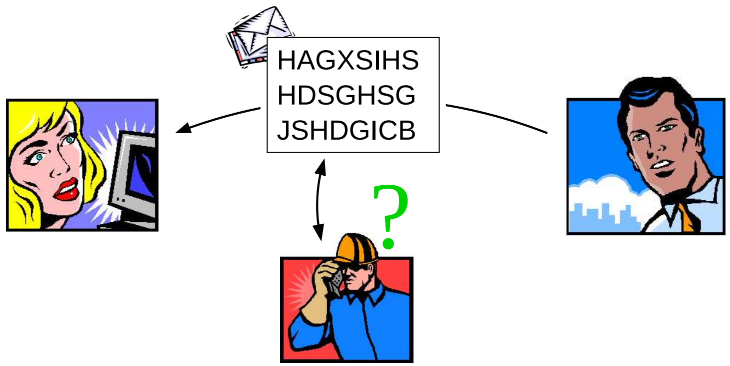
Security aspects, attacks

Basic idea of encryption



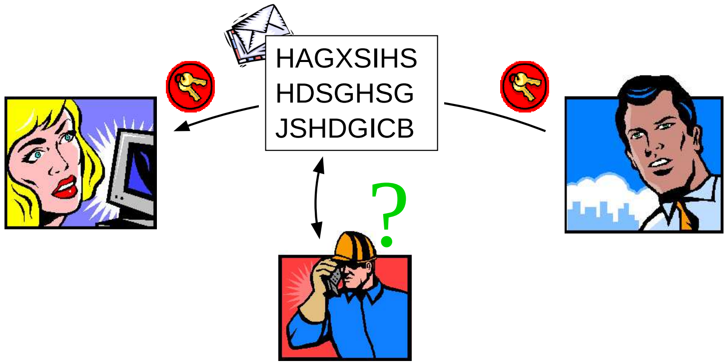
Bob wants to send Alice a message.
Oscar can eavesdrop on messages.

Basic idea of encryption



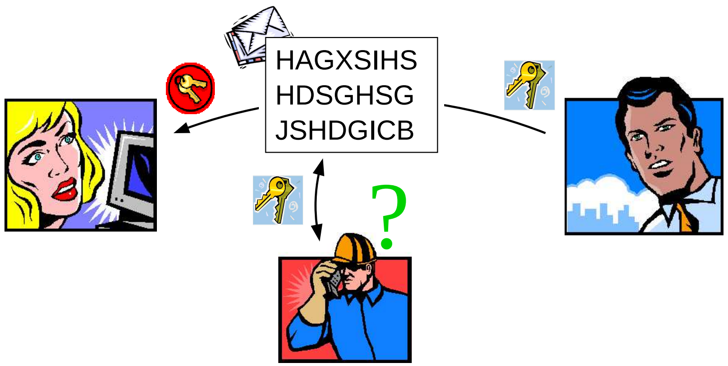
Thus the message should be encrypted.

Basic idea of encryption



Encryption and decryption with secret keys.

Basic idea of encryption



Encryption with public keys and decryption with a secret key.

Public Key Cryptography

Fundamental tasks:

- Encryption with public key and decryption with secret key.
- Signing with secret key and signature verification with public key.

Requires some sort of one way function f:

- easy to compute $f(x)$,
- hard to invert, i.e. hard to compute $f^{-1}(y)$.

Strictly speaking, such functions are not known to exist.

But there are candidate one way functions which do the job given current knowledge.

Candidate one way functions

Candidate one way functions can be obtained by computational mathematical problems, in particular from number theory.

The inverse operations are usually based on or related to

- Factoring of integers,
- Discrete logarithms in finite fields and elliptic curves over finite fields.

Other possibilities are

- Shortest and closest vectors in lattices or codewords,
- Solving multivariate equations.

Elliptic curves lead to very efficient systems compared to factoring integers and finite fields.

Integers and prime numbers

The set of integers is

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}.$$

Integers can be added, subtracted and multiplied ($+$, $-$, $\cdot$).

A prime number in $\mathbb{Z}$ is a non-negative integer which is only divisible by 1 and itself.

- Example: $2, 3, 5, 7, 11, 13, \dots, 337837575858752378528732593151, \dots$

Every integer can be decomposed into prime numbers.

- Example: $350 = 2 \cdot 5 \cdot 5 \cdot 7$.

Division with remainder

Not every division is possible in $\mathbb{Z}$: $5/3 \notin \mathbb{Z}$. There are remainders.

Division with remainder:
Let $a, p \in \mathbb{Z}$, $p > 0$. Write $a = hp + r$ mit $h, r \in \mathbb{Z}$ und $0 \le r \le p - 1$.

Then $h = a$ div p and $r = a$ mod p.

- Example: 5 div $3 = 1$ and 5 mod $3 = 2$, because $5 = 1 \cdot 3 + 2$.
- Example: -1 mod $3 = 2$, $(2 \cdot 3)$ mod $5 = 1$.

Computing modulo prime numbers

$\mathbb{F}_p := \{0, 1, \dots, p - 1\}$.

Elements in $\mathbb{F}_p$ can be added, subtracted and multiplied like in $\mathbb{Z}$ upon reducing the results modulo p.

Elements in $\mathbb{F}_p$ can be inverted and divided if and only if p is a prime number.

- Example: In $\mathbb{F}_5$ the element 2 is the inverse of 3, because $2 \cdot 3 = 6 = 1$ mod 5.

Inverses and Divisions can be easily computed using the euclidian algorithm.

Finite fields

In the following p is always a prime number and $q = p^r$ with $r \in \mathbb{Z}^{\ge 1}$.

$\mathbb{F}_p$ with this modular arithmetic is called a prime finite field.

Let $\mathbb{F}_q = \{\lambda_0 + \lambda_1 x + \dots + \lambda_{r-1} x^{r-1} \,|\, \lambda_i \in \mathbb{F}_p\}$.

Using prime polynomials, polynomial division with remainders and polynomial modular arithmetic $(+, -, \cdot, /)$ like in the integer case, the set $\mathbb{F}_q$ becomes a general finite field.

$\#\mathbb{F}_q = q$.

$\mathbb{F}_q$ can be implemented:
Operations constr, $+, -, \cdot, /, =$ etc are available.

Discrete Logarithms

Let ℓ denote a prime number with $\ell \mid \#(\mathbb{F}_q \setminus \{0\}) = q - 1$.

There is $g \in \mathbb{F}_q$ with $g^\ell = 1$ and the following property:
Every $y \in \mathbb{F}_q$ with $y^\ell = 1$ can be written in the form $y = g^x$ for exactly one $x \in \mathbb{Z}$ with $0 \le x \le \ell - 1$.

The exponent x is called discrete logarithm of y in base g.

Example:

- $3^4 = 4$ mod 7.
- $2802314782068674676625088306\,51^{4608142691076443876193757\,9795} =$ $2071505059735546984247053462\,92 \bmod 337837575858752378528732593151$.

The problem of finding x given g, y is called Discrete Logarithm Problem.

Discrete Logarithms

Let the prime power q have more than 300 and ℓ more than 50 decimal digits.

The computation of g^x given g and x is „easy“.
The computation of x given g and g^x is „very hard“.

The exponentiation function $x \mapsto g^x$ is a candidate one way function.

The discrete logarithm problem is the same as inverting the exponentiation function.

ElGamal Encryption

1. Key generation done by Alice:

: Is random, secret x with $0 \le x \le \ell - 1$.

: Is $y = g^x$. $\longrightarrow$ y

Messages: Represented as elements $m \in \mathbb{F}_q \setminus \{0\}$.

2. Encryption done by Bob: Chooses random, secret $r \in \mathbb{Z}$.
Computes (g^r, my^r).
$(u, v) \longleftarrow (g^r, my^r)$.

3. Decryption done by Alice:
Computes vu^{-x}. Then $vu^{-x} = mg^{xr}g^{-rx} = m$.

Abstraction

What has been used so far? Computing in $\mathbb{F}_q$, but only multiplication and inversion, no addition or subtraction or zero element!

A set G, in which elements can be multiplied and inverted in a „sensible“ way, is called a group.

ElGamal encryption works in principle in every group
in which the elements can be represented in the form g^x.

Question: Are there further well suited groups except $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$?

Answer: Yes, elliptic curves!

Elliptic curves

Let $q = p^r$ large with $p \geq 5$ and $a, b \in \mathbb{F}_q$ suitable.

An elliptic curve is given by an equation: $E : Y^2 = X^3 + aX + b$.
Points on the elliptic curve $E(\mathbb{F}_q) = \{(x,y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + ax + b\} \cup \{O\}$.

Slightly different equation for $p = 2, 3$ but otherwise analogous.

There are special formulae by which points $P, Q \in E(\mathbb{F}_q)$ are „multiplied“. The point O is the neutral element.

For historic reasons multiplication is written as addition $P + Q$ and exponentiation by $x \in \mathbb{Z}$ as multiplication xP.

Elliptic curves

Let $q = p^r$ large with $p \geq 5$ and $a, b \in \mathbb{F}_q$ suitable.

An elliptic curve is given by an equation: $E : Y^2 = X^3 + aX + b$.
Points on the elliptic curve $E(\mathbb{F}_q) = \{(x,y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + ax + b\} \cup \{O\}$.

Slightly different equation for $p = 2, 3$ but otherwise analogous.

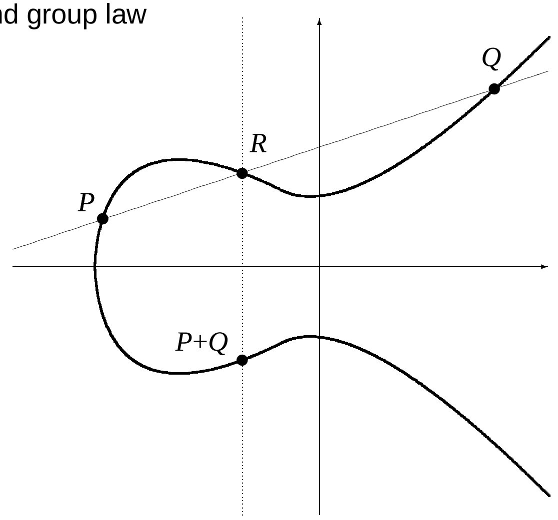
There are special formulae by which points $P, Q \in E(\mathbb{F}_q)$ are „multiplied“. The point O is the neutral element.

For historic reasons multiplication is written as addition $P + Q$ and exponentiation by $x \in \mathbb{Z}$ as multiplication xP.

$E(\mathbb{F}_q)$ can be implemented:
Operations constr, $+, -, \cdot, =$ etc are available.

Elliptic curves

Curve and group law



Discrete Logarithms

Let ℓ denote a prime number with $\ell \mid \#E(\mathbb{F}_q)$.

There is $P \in E(\mathbb{F}_q)$ with $\ell P = O$ and the following property:
Every $Q \in E(\mathbb{F}_q)$ with $\ell Q = O$ can be written in the form $Q = xP$ for exactly one $x \in \mathbb{Z}$ with $0 \leq x \leq \ell - 1$.

The exponent x is called discrete logarithm of Q in base P.
The problem of finding x given P, Q is the ECDLP.

Hardness of the DLP

It is believed that the most efficient method for solving a random ECDLP in $E(\mathbb{F}_q)$ for random $a,b \in \mathbb{F}_q$ cannot take advantage of the special structure of E and hence requires at least $\approx \ell^{1/2}$ steps.

In other words it is expected that such an ECDLP has maximal security in group based cryptography, in relation to the group size $\#E(\mathbb{F}_q)$.

Elliptic curves have been proposed for cryptographic use in 1986.

The time for solving the DLP in $\mathbb{F}_q^\times$ is more like $\min\{\ell^{1/2}, \exp(c\log(q)^{1/3})\}$.

Comparison

Comparison of key sizes for roughly equal security.

Block cipher key size	Example block cipher	ECC key size	RSA / $\mathbb{F}_q^\times$ key size
80		163	1024
112	3DES	233	2048
128	AES	283	3072
192	AES	409	7680
256	AES	571	15360

ECC with 517 practical, but RSA or $\mathbb{F}_q^\times$ with 15360 not.

Problems and questions

with respect to security and practicability.

1. How construct E with $\ell | \#E(\mathbb{F}_q)$ („point counting")?
2. Special cases where ECDLP is easy?
3. Optimisations of speed/memory usage (e.g. „point compression").

Construction of suitable elliptic curves

Have $\#E(\mathbb{F}_q) = q+1-t$ where $|t| \le 2\sqrt{q}$ unknown.
Need to know $\ell | \#E(\mathbb{F}_q)$.

Random E: Randomly choose $a,b \in \mathbb{F}_q$. Compute $\#E(\mathbb{F}_q)$.
Subfield E: Choose $a,b \in \mathbb{F}_p$. Write down $\#E(\mathbb{F}_q)$ using $\#E(\mathbb{F}_p)$.

Check $\ell | \#E(\mathbb{F}_q)$ by trial division of small factors and primality test.

Complex multiplication E: Construct E with known $\#E(\mathbb{F}_q)$.

The subfield and complex multiplication constructions yield curves with more mathematical structure than random curves. This could potentially be useful for an attack ...

Insecure cases

Multiplicative transfer (Frey-Rück reduction, Menezes-Okamoto-Vanstone attack, 1991).

Assume $\ell \mid (q^k - 1)$ with $k \geq 1$ minimal.
It is possible to efficiently transfer the ECDLP into a DLP in $\mathbb{F}_{q^k}^{\times}$.

The DLP in $\mathbb{F}_{q^k}^{\times}$ is still quite hard.

For random and independent q and ℓ: $\log(k) \approx \log(\ell)$.
For supersingular elliptic curves ($t = 0 \bmod p$): $k \leq 6$!

Random and independent case no problem, but supersingular elliptic curves much weaker than generically expected.

Are still useful, for example in identity based cryptography.

Insecure cases

Additive transfer (Rück or SmartASS attack, 1997).

Assume $\ell = p$ (anomalous or trace one curves).
It is possible to efficiently transfer the ECDLP into a DLP in $\mathbb{F}_p^{+}$.

The DLP in $\mathbb{F}_p^{+}$ is very easy.
Hence the case $\ell = p$ is totally insecure.

Insecure cases

„Weil descent methodology“ or „covering attacks“ (Gaudry-Hess-Smart, Diem, 2000-3)

$q = 2^r$, $k = \mathbb{F}_q$, $K = \mathbb{F}_{q^n}$, E elliptic curve over K.

An algebraic curve C_0 defined over k is constructed such that the ECDLP in $E(K)$ can be efficiently transferred to a DLP in $\mathrm{Pic}_k^0(C_0)$.

Under certain circumstances the DLP can be solved faster in $\mathrm{Pic}_k^0(C_0)$.

Security reduction possible if $n \geq 3$ is small or medium.

Insecure cases

Index calculus attack via summation polynomials and Weil restriction (Semaev, Gaudry, Diem, 2004).

Introduces a size notion on points in $E(\mathbb{F}_{q^n})$ such that points decompose into a small number of „small“ points (like a prime factorisation) ...

The ECDLP in $E(\mathbb{F}_{q^n})$ can be computed in time $O(q^{2-2/n})$ for fixed n and $q \to \infty$ instead of $\ell^{1/2} \approx q^{n/2}$.

The ECDLP might even be computed much more efficiently if $n \approx \log(q)$ grow together.

The ECDLP for small or medium $n \geq 3$ for general q may be weaker than expected!

Avoiding insecure cases

The last two attacks do not yield such a strong security reduction like the multiplicative transfer, let alone the additive transfer.

Any of these attacks can be easily avoided, for example:

- Use random elliptic curves E.
- Use only prime fields $\mathbb{F}_p$, or extension fields $\mathbb{F}_{p^r}$ with r a big prime and p small, for E.

If you cannot use your own elliptic curve, maybe you can use a curve created verifiably at random:

- a, b are given via cryptographic hash values of two published numbers ...

Conclusion

Elliptic curves can be used to implement group based cryptography.

They provide a very high efficiency / security ratio.

Research in possible attacks is still actively carried out.

The known attacks can be quite easily avoided using random elliptic curves over suitable finite fields.

Quantum computers are bad for group based cryptography and RSA.