ALICE, BOB AND ELLIPTIC CURVES

SAM MARSH

ABOUT THE TALK

The talk concerned the sending of messages securely between two parties, Alice (A) and Bob (B) say, in such a way that an unwanted eavesdropper, Eve (V), cannot gain any information.
Two main approaches were highlighted: *steganography* (where the existence of the message is hidden) and *cryptography* (where the meaning of the message is obscured). The talk concentrated on the latter.

The main idea was to turn a plain text message into a cipher text (or disguised) message.

The method was to break the text into message units, and transform each one into a different message unit via an *enciphering transformation*: an invertible map $f : P \to C$, where P is the set of plain text message units, C is the set of cipher text message units.

A set-up such as this is referred to as a *cryptosystem*.

1. Symmetric Cryptosystems

A straight forward example was given where

$$P = C = \mathbb{F}_q \text{ for some } q$$

. The function $f : P \to C$ has the form

$$f(x) = ax + b$$

where

$$a \in \mathbb{F}_q^\times \text{ and } b \in \mathbb{F}_q$$

are fixed. This is a bijection by invertibility of a (explicitly,

$$f^{-1}(y) = a^{-1}y - a^{-1}b$$

). The parameter pair $K_e = (a, b)$ is known as the **enciphering key** for the enciphering transformation, while the pair $K_d = (a^{-1}, -a^{-1}b)$ is known as the **deciphering key**. A system where knowing K_e essentially means knowing K_d is called **symmetric**. Symmetric cryptosystems are good ways of transferring information as they usually don't increase the amount of information being transmitted too much. However, it is very important that both K_d and K_e remain secret. Often this will mean a meeting will need to take place, which is not always feasible.

Too much display-math

2. Public Key Cryptography

The next example of a cryptosystem was *Public Key Cryptography*. Suppose the form of f is known but K_d is difficult to calculate from K_e. This leads to a function f which is difficult to invert (a *trapdoor function*). The system then works as follows:

- B knows K_e and K_d for a trapdoor function and publishes K_e.
- A encrypts a message using K_e.
- Since only B knows K_d, only he can decode the message.

An example of this is the RSA system, which relies on the fact that a product of two large primes is difficult to factorise if neither of the primes are known.

Diffie-Hellman Key Exchange

As mentioned above, symmetric cryptosystems are good ways of transferring information but rely on a key having already been agreed. The *Diffie-Hellman Key Exchange* was described as a way of securely agreeing on a key without needing to meet. The security of the exchange relied on the *discrete logarithm problem* (viz. given a finite group G, an element $a \in G$ and $k \in \mathbb{N}$, how can we find k knowing only a and a^k?) being difficult to solve if G is large. The procedure is as follows:

- B fixes a finite field $\mathbb{F}_q$ and an element $g \in \mathbb{F}_{\shortparallel}^{\times}$ He sends this information to A.
- A chooses an integer $1 \leq a \leq q-1$ and sends g^a to B.
- B chooses an integer $1 \leq b \leq q-1$ and sends g^b to A.
- A and B now both know $g^{ab} = g^{ba}$, and this is used as a key for a cryptosystem.

This is secure: if V "overhears" g, g^a and g^b then she can't form g^{ab} without solving the DLP. Hence, if B has chosen q such that the DLP is hard in $\mathbb{F}_q$ then V won't be able to find the key easily. A and B can then use the key in a symmetric cryptosystem.

Massey - Omura Cryptosystem

The procedure for this system (illustrated by sending the message $p \in \mathbb{F}_q$) was described as follows:

- B fixes $\mathbb{F}_q$ and sends to A as before.
- A and B each select an integer $1 \leq e_* \leq q$ such that $\gcd(e, q-1) = 1$.
- Put $d := e^{-1}$.
- A sends p^{e_a} to B.

- B sends $p^{e_a e_b}$ to A.
- A sends $p^{e_a e_b d_a} = p^{e_b}$ to B.
- B then knows p, and the message has been transferred.

This is not secure: if V pretends to be B she can access the information. Some kind of signature system needs to be incorporated to prevent this. Note that if the DLP is hard in $\mathbb{F}_q$ then B can't deduce e_a, so this will be kept secret. Also V will find it difficult to gain any information by simply eavesdropping: DLP again.

Elliptic Curves

Elliptic curves can be used to create cryptosystems. The additive abelian group $E(\mathbb{F}_q)$ defined in the usual way is a good example of a group for which the DLP is hard, and hence works well for the Diffie-Hellman Key Exchange. Some attacks that work on Finite Field Cryptosystems do not carry over to Elliptic Curve crytposystems. They also have advantages in that often the key size is smaller with the same security.