ALICE, BOB AND ELLIPTIC CURVES

A. N. STUDENT

1. 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 $f\colon P \to C$, 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.*

2. Symmetric Cryptosystems

A straightforward example was given where $P = C = \mathbb{F}_q$ for some q. The function $f\colon p \to C$ has the form $f(x) = ax + b$ where $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$ are fixed. This is a bijection by the invertibility of a. Explicitly, we have

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

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.