**One-time Pads**

**One-time pad** is a type of encryption which has been proven to be impossible to crack if used correctly.

* Each bit or character from the plaintext is with a character from a secret random key (or pad) of the same length as the plaintext, resulting in a coded message.
* If the key is truly random, with a **size >= than plaintext**, **never re-used in whole or part** and **kept secret**, the coded message will be impossible to decrypt or break without knowing the key.

**XOR: Exclusive-Or binary operator**

* It is something that can be done really fast with minimal computing power
* XOR jumbles things up
* If you XOR number A with number B, if either of the numbers are random then the output is random.

**One-Time Encryption**

* Encrypting “I love you” (8 characters) with 1, 5, 7, 13, 8, 2, 6, 4.
* ENCODED MESSAGE: J – Q – V – I – M – A – U – Y
* If **the key was thrown away (hence ONE-TIME PAD)**, it would be impossible to crypt-analyse this encoded message to get the plaintext
* Any cipher text can correspond to any plain text.
* Things like Entropy / English language patterns become completely irrelevant

**One-time pad problems**

* It’s based on a secret
* Key distribution / distributing the one-time pads