Contents

1 Crytography

2 Encryption

- Encryption: We encode a message such that only authorised users may read it
- Cipher: takes a string of plaintext, and converts it into a string of ciphertext
- Encryption can provide: Confidentiality, Integrity, Authenticity

3 Notation

- A *cipher* converts a plaintext message **M** into a *ciphertext* **C** under the control of a key **K**
- C is **not a secret**, but without knowledge of the key, it should be impossible to **reconstruct** M
- Comes in two forms: *Symmetric* same key for encryption / decryption. *Asymmetric* separate keys

4 The One Time Pad

Using XOR to encrypt the message:

- Use a key thats the **same length** as the message
- XOR each message bit with each key bit
- Any possible plaintext can be recovered depending on the key
- This is an example where $M = C - K mod 26$

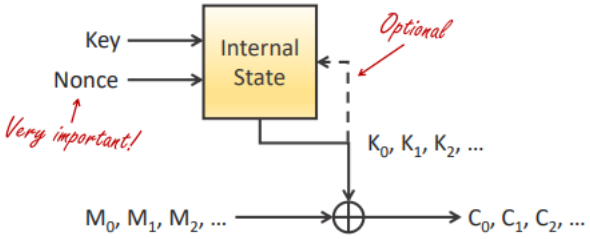
C	MXFLCRDH	MXFLCRDH
K	emrqytpn	eqfsytpn
M	iloveyou	ihateyou

It is an impractical method because:

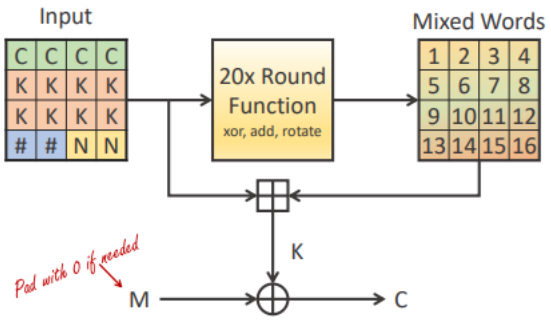
- A 1GB file would need a 1GB key!
- How are we transporting these keys? Or storing them?
- If you ever reuse a key, the entire cipher is broken

5 Modern Stream Ciphers

- Modern stream ciphers use an initial seed key to generate an infinite pseudorandom keystream
- The message and keystream are usually combined using XOR - - which is reversible if applied twice
- Common to seed an initial state using a key, then update this state for as long as needed



5.1 ChaCha20



- ChaCha performs 20 rounds: alternates Column and Diagonal Rounds, each round is 4 quarter rounds
- It's fast, because ChaCha20 is based on ARX (Addition-Rotation-XOR) which are **CPU friendly instruction**

5.2 Advantages of Stream Ciphers

- Encrypting long continuous streams, possibly of unknown length
- E.g. GSM mobile communications
- Extremely **fast with a low memory footprint**, ideal for low-power devices
- If designed well, can seek to any location in the steam. E.g. Streaming video with DRM

5.3 Vulnerabilities

- Stream ciphers give us confidentiality, but not integrity
- We must include another mechanism

Reference section

placeholder