**Network Security: Introduction**

**Breaking encryption schemes**

**Cipher-text only attack:** Analyse the cipher-text to decrypt the message.

Approaches: **Brute Force** or **Statistical Analysis**

**Known plaintext attack**: Know the plaintext and match it with ciphertext

**Chosen plaintext attack**: Get the ciphertext for a chosen plaintext

**Symmetric Ciphers**

**Stream Ciphers**

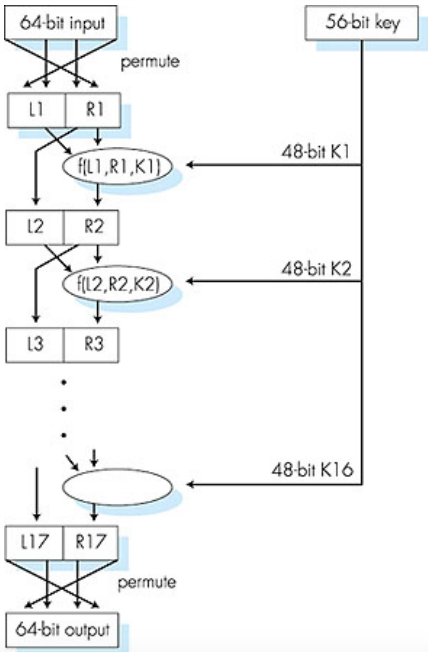
Combine plaintext with pseudorandom cipher (similar behaviour as the One Time Pad)

**RC4 Stream Cipher**: A popular stream cipher used in WEP for 802.11 / can be used for SSL.

**Block Ciphers**

Ciphertext processed from plaintext as **k bit blocks**.

**Data Encryption Standard (DES)**



DES is a **block cipher** with **cipher-block chaining.**

How secure?

* 56-bit-key encrypted phrase decrypted (brute force) in less than a day. No good known analytical attack.

How to make it more secure?

* **3DES:** encrypt 3 times with 3 different keys.

**DES Operations:**

1. Initial permutation
2. 16 identical rounds of function application, each using different 48 bit keys
3. Final permutation

**Advanced Encryption Standard (AES)**

Symmetric-key standard, replaced DES in 2001.

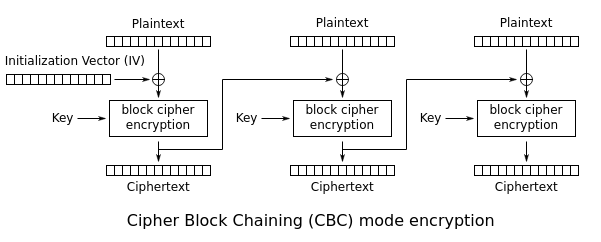
Processes data in **128 bit blocks.**

**128, 192 or 256 bit keys**.

Brute force decryption, taking 1 second on DES, takes 149 trillion years for AES.

**Cipher Block Chaining (CBC)**

Split plain text into multiple blocks, then use ciphertext of the previous block XOR with the current plaintext (for the first block XOR with Initialization Vector (IV) instead).



If the first block has index 1:  
  
The mathematical formula for **CBC encryption** is:

https://lh4.googleusercontent.com/VXIb-d0DRRCfyFLZx25Xn9wBZ_Tjg2iAGfjrsHgaW6pBlOxvh0RRc-OLJ_MLTiB3njkJil_kUCmWWF0Dyh9K1AnpgQYycwjlJQJL6dyrOT_FixTZdz-N7PerXPLtqmPSF7V-K-XE

https://lh4.googleusercontent.com/qieIWrmFKa_PuSmKeMsLKBblekM5WnFdBM9qnqzkaOSjHhrR3pnd3_XeIYEuwnKkfMKl2pjNPhlgG6Km8pHSy4Fwy_rIPxsxEsC8fv6u3F3KgIIhkgzU1040M1lPEWD5mrNFLap-

The mathematical formula for **CBC decryption** is:

https://lh6.googleusercontent.com/5AR3yp_MKA1Dziiu1EPSAJhd2gz0h0S4o0eBEF59mwqxzS3xlBlvX85SnDe_MEi2Wzk_KvyNY3AxVFWqsi-tOfCPfLHRb3plssUBz7wCUP-L-XvdZXjMZ8quRIK0hsTpfKx0mk_c

https://lh3.googleusercontent.com/IaJd_eorvq68yvem5zl9FRw7nSTiV0GlLINTRJuT7FwzIyxoh5u1NM3p6ohE3D5d60xYeH2P1TtiCteaxv5xql82q2QyQfqZ_4NyYJIZyBguzc2SbwIpjoIKMYiyfK9zLIIilj-C

