Network Security Contd

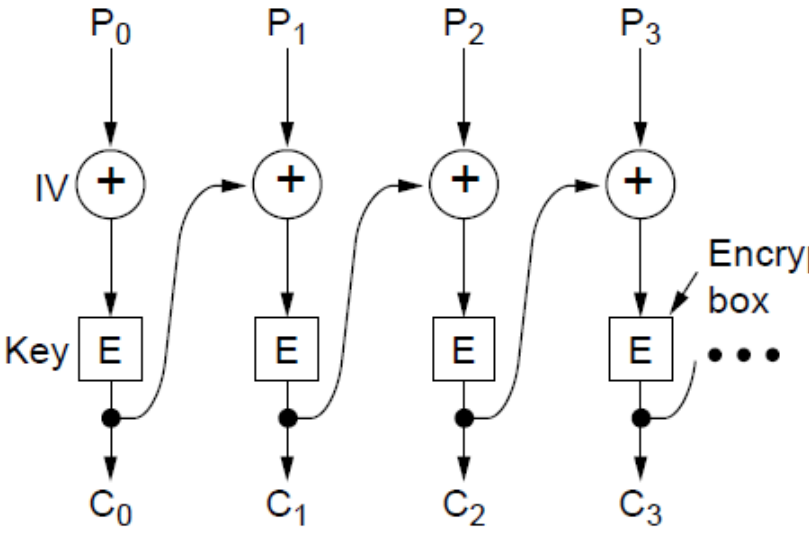
Internet Technologies
COMP90007

Modern Key-based Algorithms

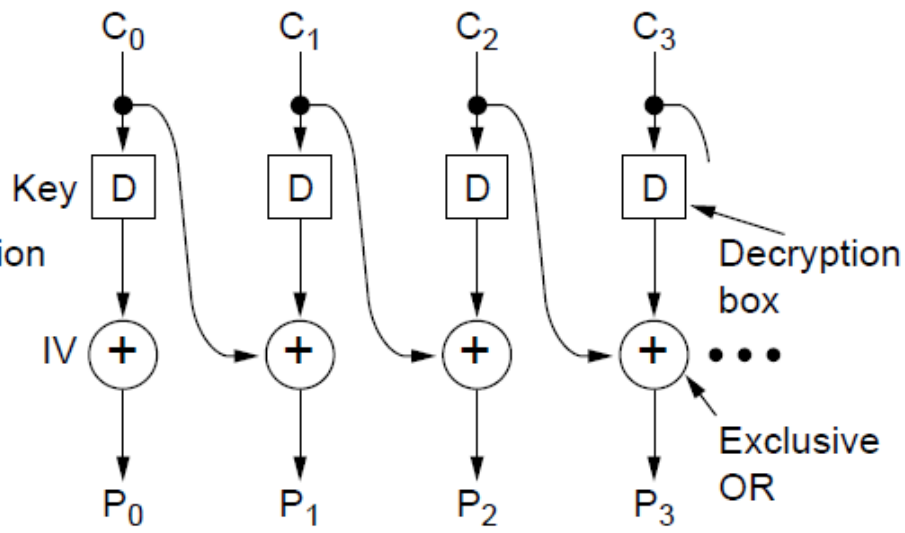
- **2 Examples of Symmetric Key Algorithms from real life**
  - Data Encryption Standard (DES)
    - Uses 64 bit blocks and 56 bit keys
    - 2^{56} key space
    - Triple DES has a 3 x 2^{56} key space
  - Advanced Encryption Standard (AES) in use since 2000s
    - Uses 128 bit blocks and 128 bit keys
    - 2^{128} key space
    - **Still substitution and permutation based** with multiple rounds

Cipher Block Chaining Mode

- Over time people created many ways to substitute + permute input data and more ways are to be invented but…
- **Same text leads to same ciphertext unless something else is done, thus…**
- People invented **block chaining mode**, each plaintext block is XOR'ed with the previous ciphertext block before being encrypted



CBC mode encryption



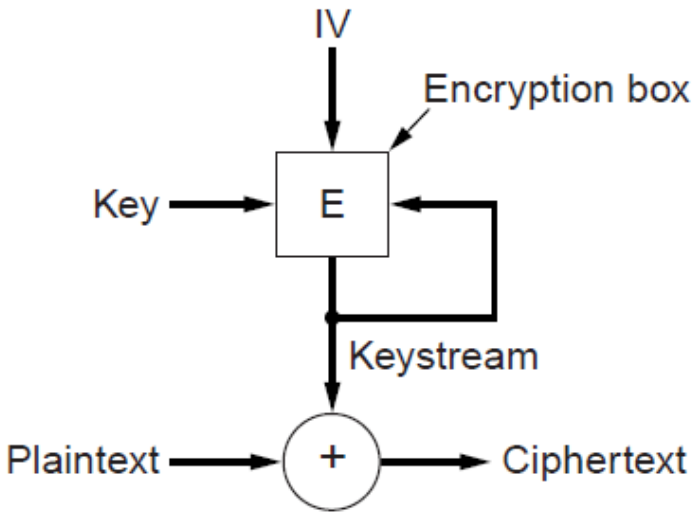
CBC mode decryption

Cipher Feedback Mode

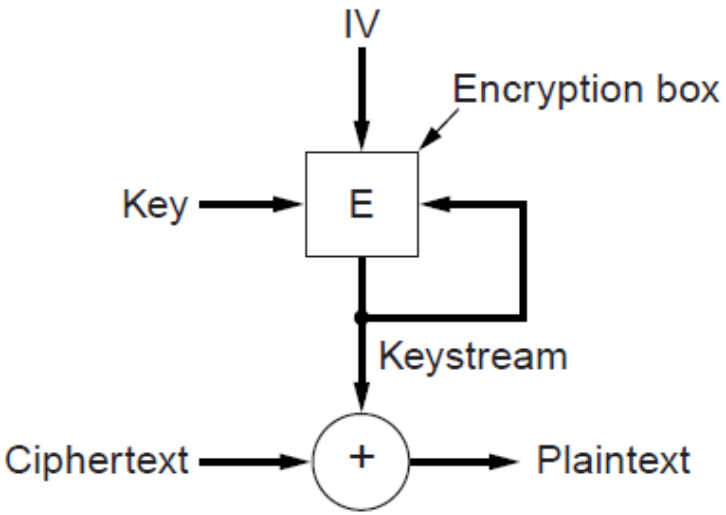
- In cipher feedback mode, **byte-by-byte encryption** is used rather than block-by-block encryption
- Simple upgrade but important for some apps
- Good for things like encrypting someone's key strokes on a keyboard **where a lot of data is not immediately available**

Stream Cipher Mode

- What if **data transmission errors occur**? One can loose the whole lot
- We need to have an upgrade that is not receptive to such errors
- In stream cipher mode, recursive sequential block encryption is used as a **one-time pad**, and XOR'ed with plaintext to generate ciphertext



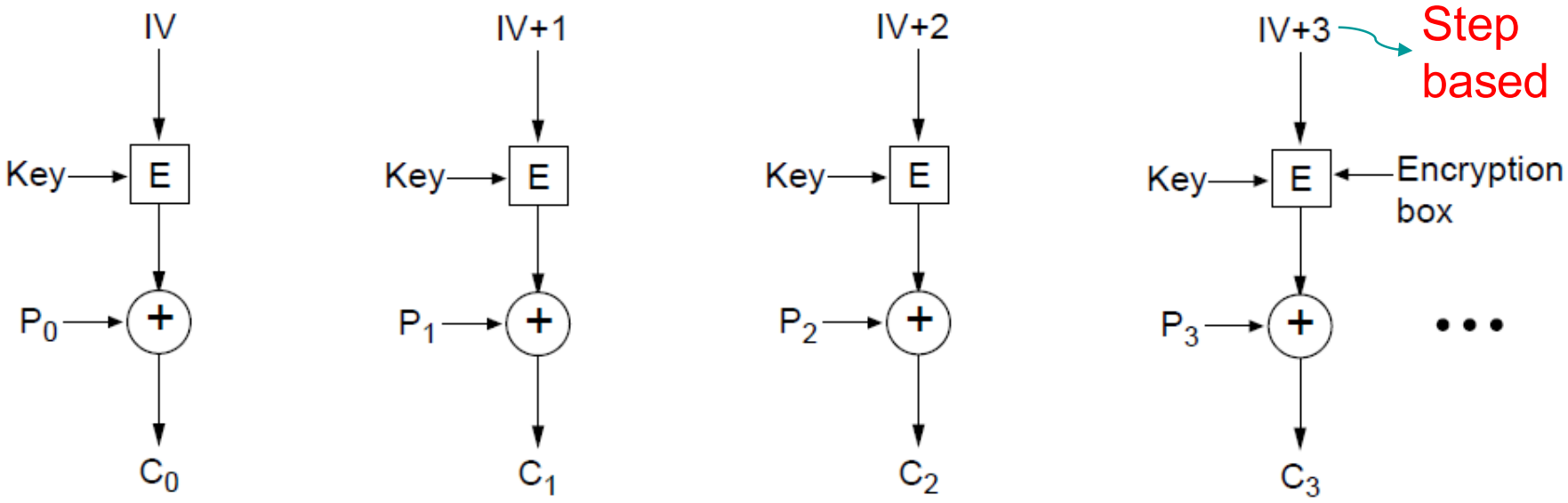
Encryption



Decryption

Counter Mode

- But **how about random access to data after encryption**?
- In counter mode, plaintext is not directly encrypted, but an initialisation parameter plus an arbitrary constant is encrypted, and the resulting ciphertext is XOR'ed with plaintext



Many Symmetric Key Algorithms Exist…

Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Second best choice
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

Second Category: Public Key Algorithms

- Fundamentally different to symmetric key ones
- Diffe & Hellman proposed the new model
  - **Relies on asymmetry**
  - **Two keys are used**
  - Important: Keys not easily derivable from each other
  - Hence addressing a fundamental issue: *key sharing*

Asymmetric Keys

- Diffe-Hellman key system
  - **Key 1: public key**, usable by anyone **to encrypt** messages to the owner of the key, this key known to all
  - **Key 2: private key**, required **to decrypt** the message and known only by the owner of this key, if you tell this key to someone else, it is basically your fault, the algorithms here do not require this key to be told to anyone for them to work

The Process is the Same

- C = ciphertext, P = plaintext, E = encryption, D=decryption and **K1, K2 are the keys**
- $C = E_{K1}(P)$
  - Sender knows the public key K1 and the P
- $P = D_{K2}(C)$
  - Only receiver knows private K2 which can undo K1's effect
- $D_{K2}(E_{K1}(P)) = P$

Example: RSA Security

- RSA's security is based on the difficulty involved in factoring large numbers
- Fundamentals came from number theory – inventors were from MIT and won the Turing Award in 2002
- How good it is: no one figured out a way to break it in many decades now
- Brute force breaking it >> Approx. 10^{16} years
- Disadvantage: RSA is too slow as keys are 1024 bit among other things

RSA Security Contd

- …but is widely used for many other things such as **secure key distribution**

- … then one can do RSA in tandem with faster symmetric key algorithms…