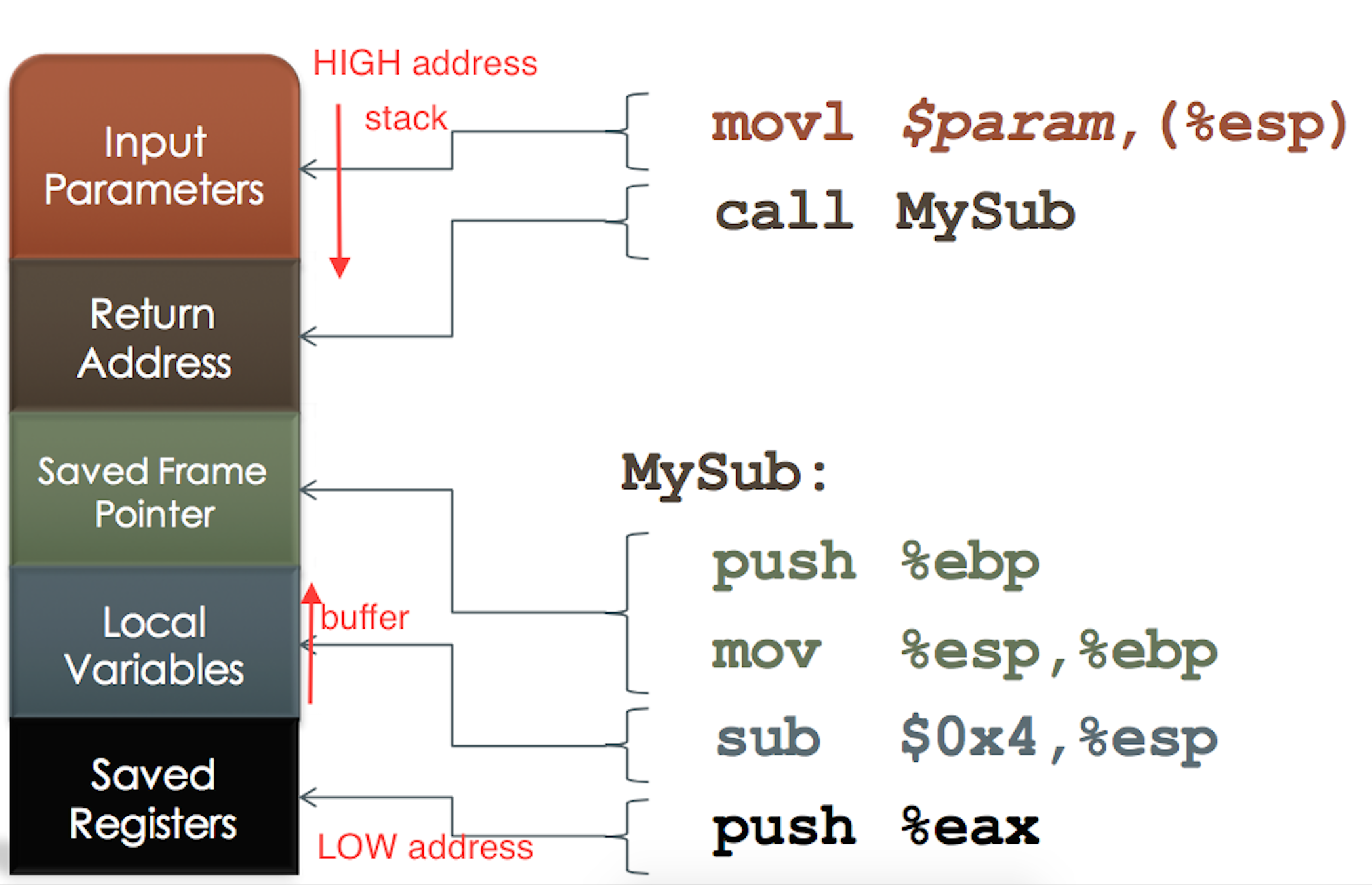
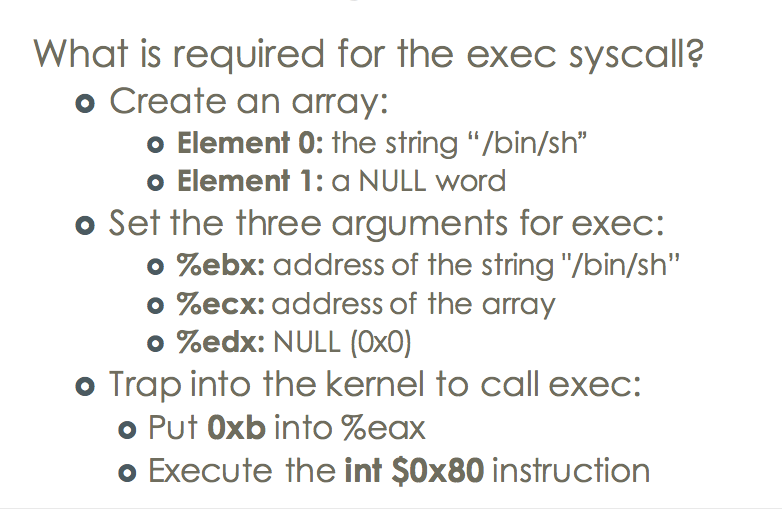
­

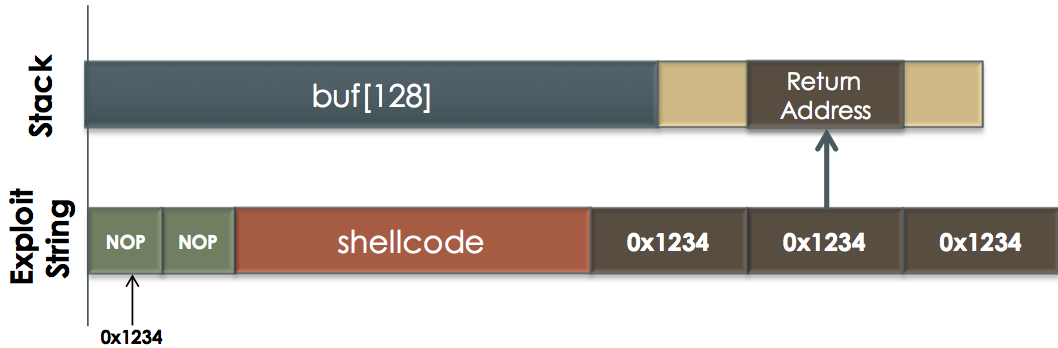
**1, buffer**

**Stack layout**

****

**Optimizing the Shellcode**

****

**Creating an exploit:**

WhyNop1,we do not know the exact address of buf

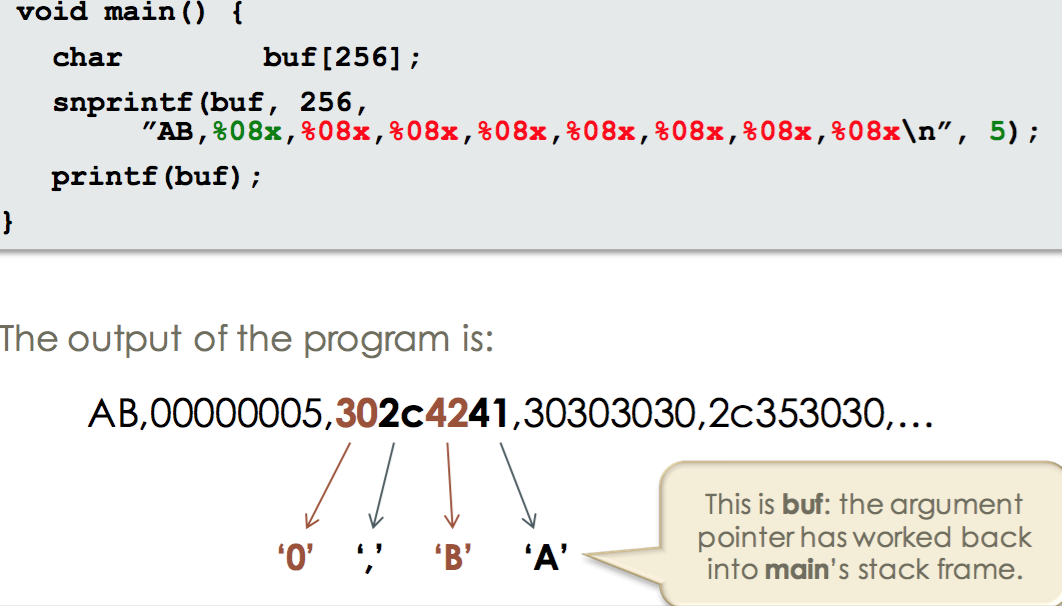
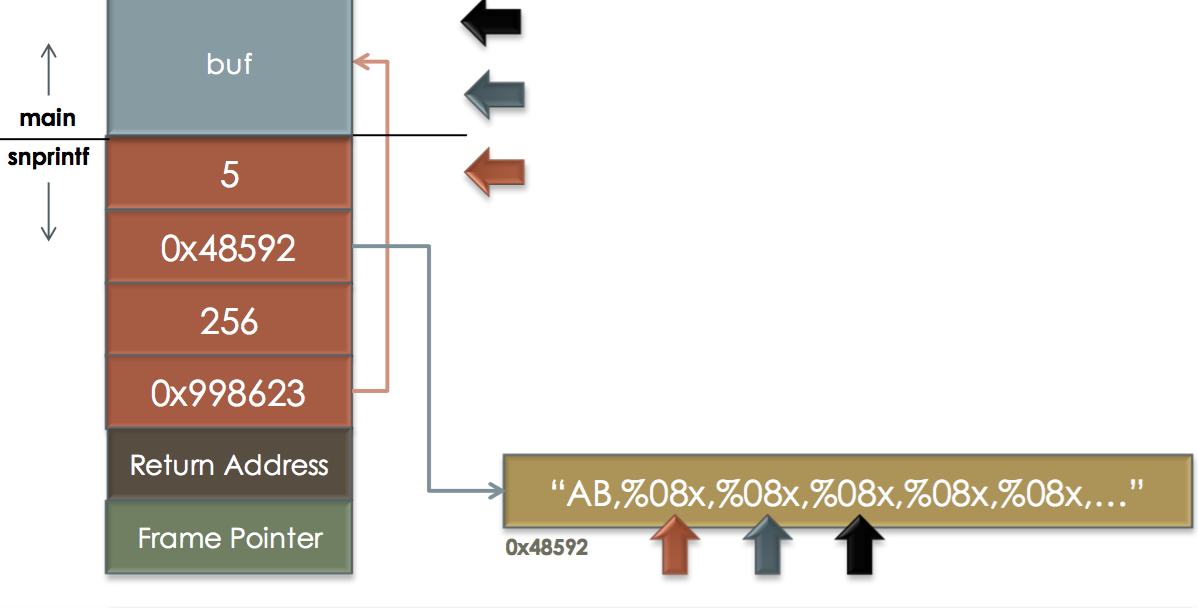
2, CPU can skip thos instructions

3, better range to guess and trap into the system

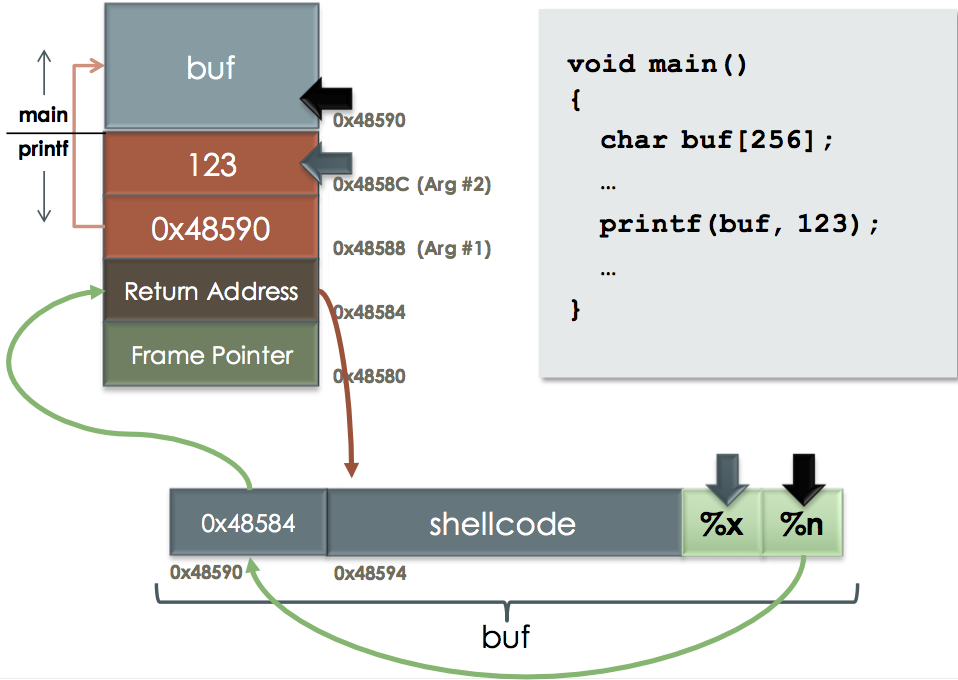
**Same direction buffer and stack overflow:**

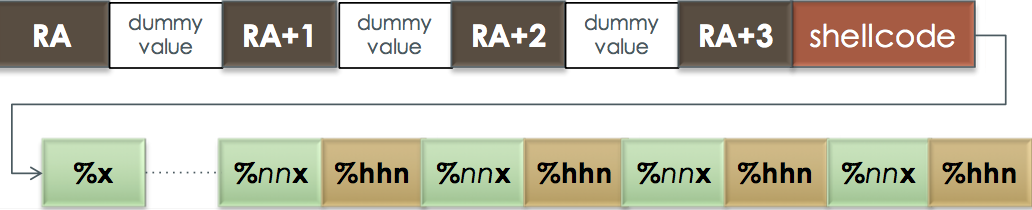
**Local variable stack layout**

**Snprintf operation**

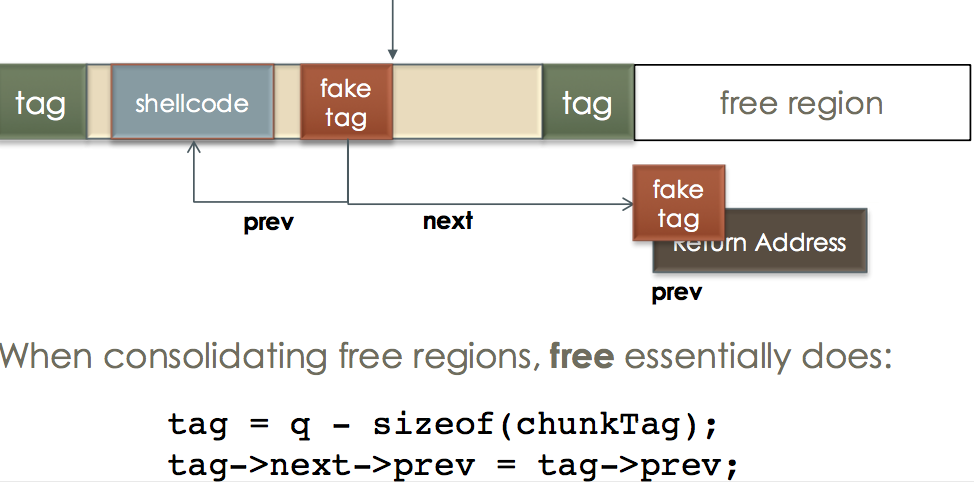
****

Format string attach

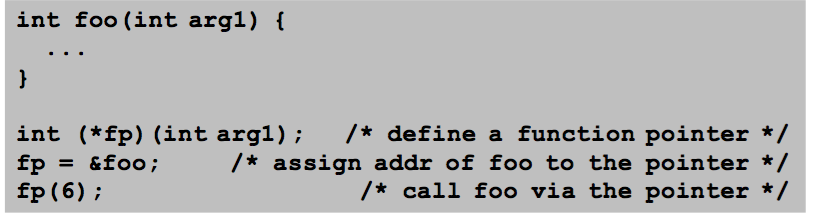


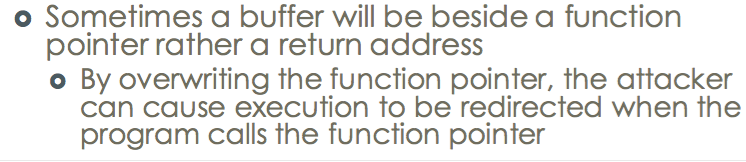
Overwritten the return address

Double free

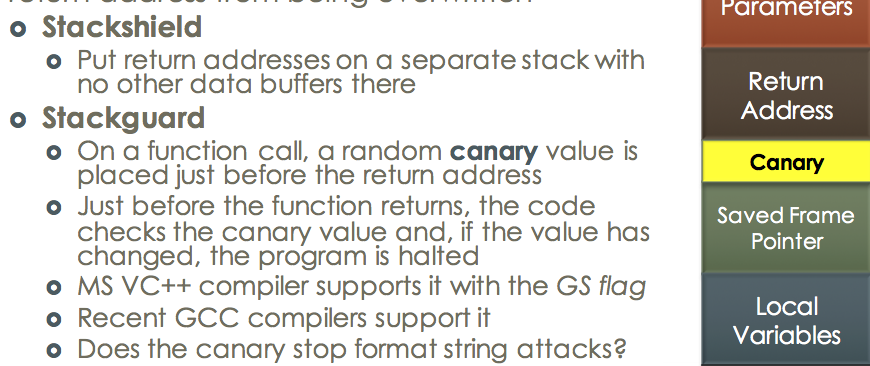


Funtion Pointers

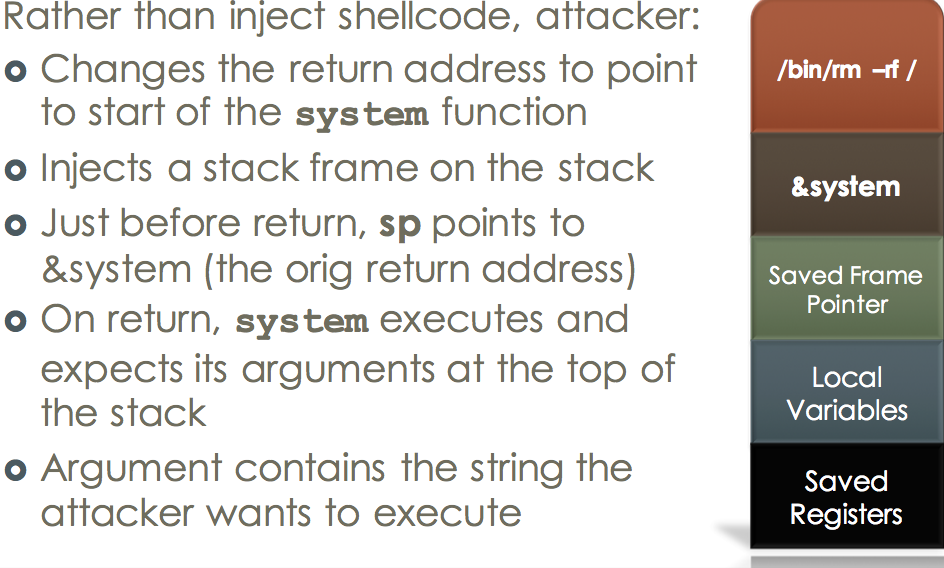




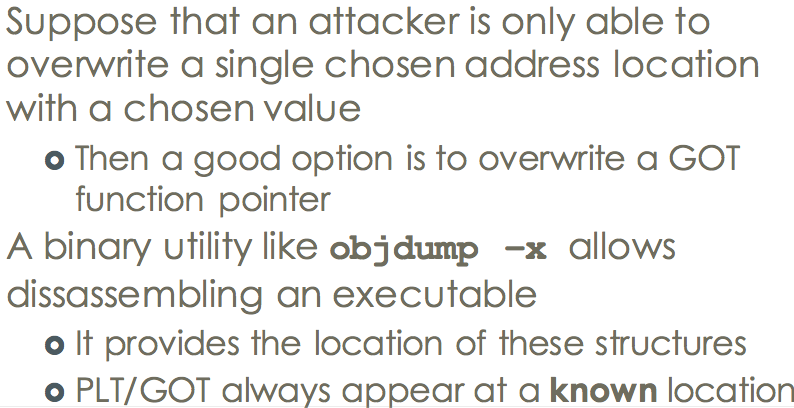
Defending Against Stack Smashing



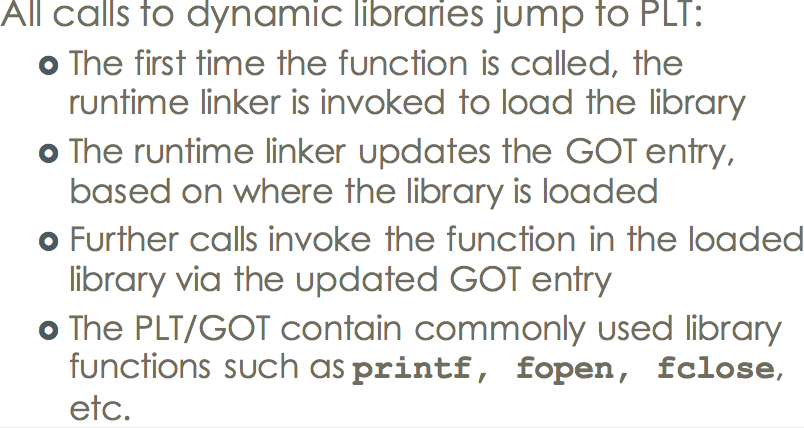
Return into libc



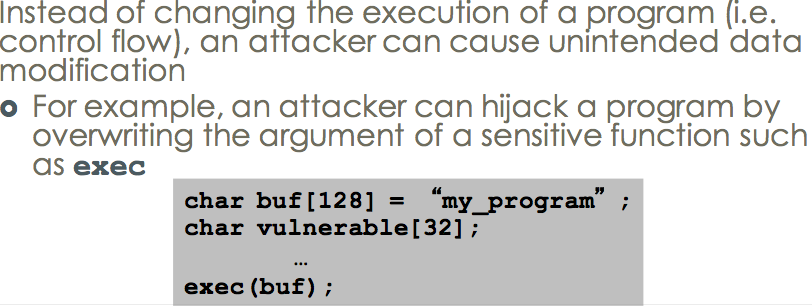
PLT/GOT



Dynamic link

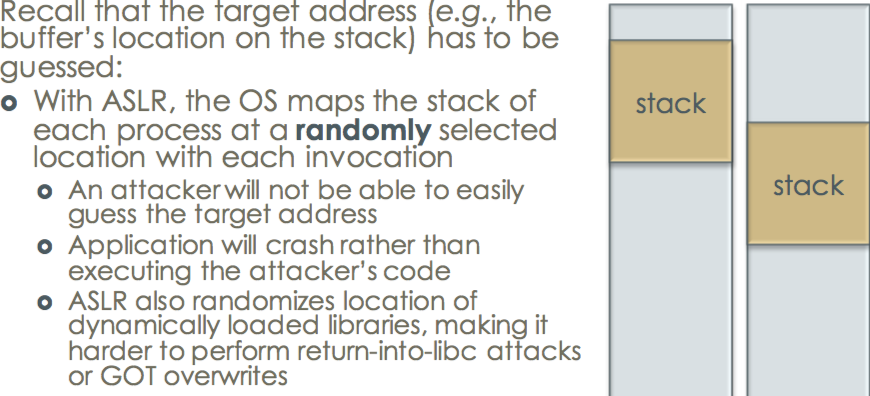


Argument overwrite

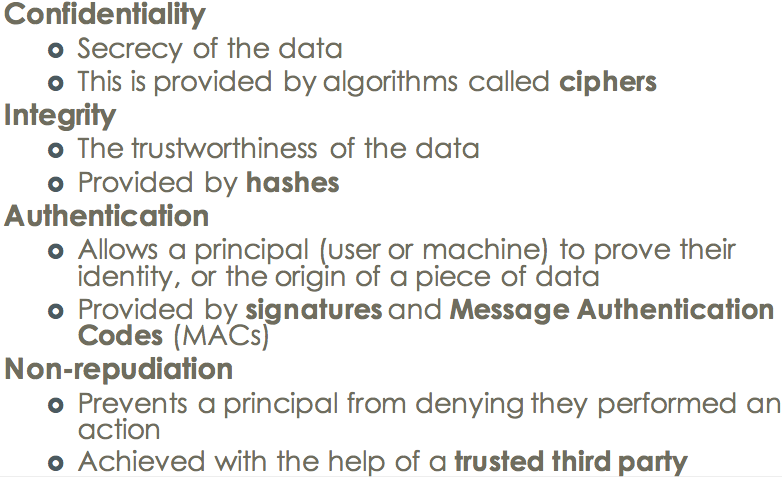


Address-Space Layout

Randomization (ASLR)



properties of Cryptography



Cryptography kinds

1, Ciphertexts

2, Number of plaintext and ciphertext pair

3, pick a plaintext and get corresponding ciphertext or

vice-versa

Polyalphabetic Cipher

One-time pad problem

1, Key length = message length

- Key overhead of 100% is generally not acceptable

2, Each key can be used once (hence the name)

3, Cipher is malleable

4, Ciphertext-only:

- If used properly, impossible to break

5, Known-Plaintext ›

- Very weak ›

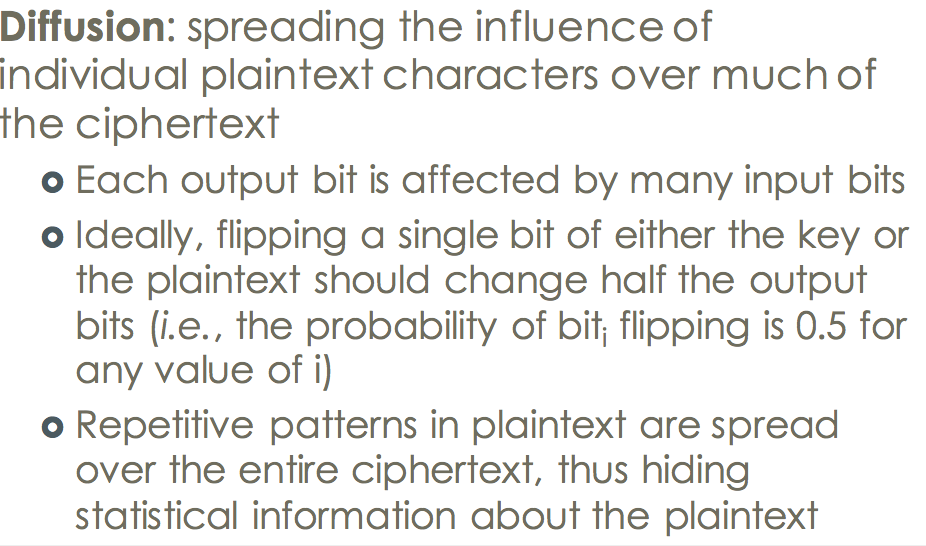
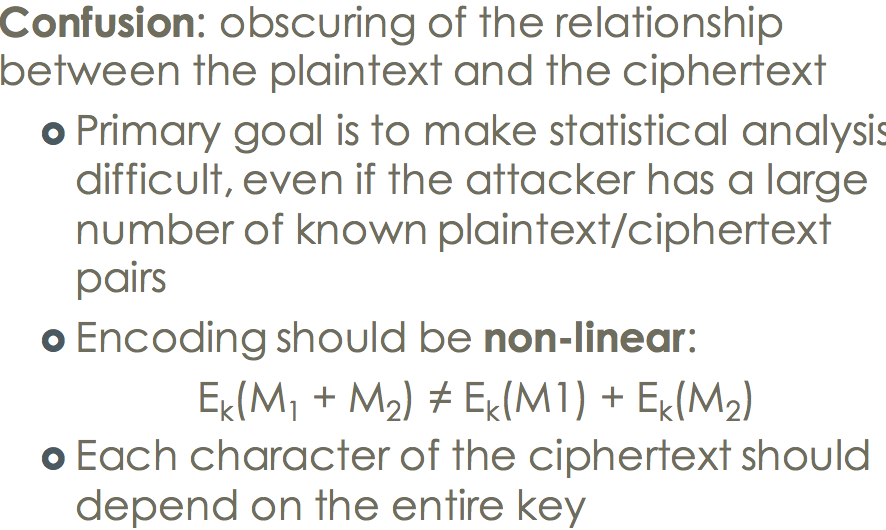
- just XOR CT with PT to reveal the key ›

- Only need one pair ›

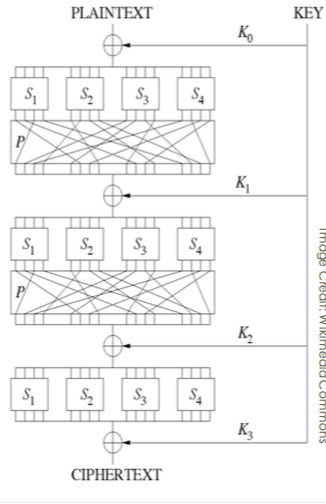
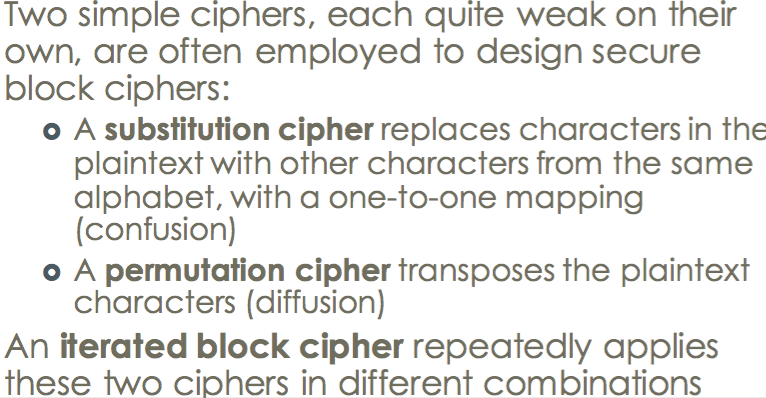
- Of course, key is not supposed to repeat

6, Chosen-Ciphertext/Plaintext -> weak

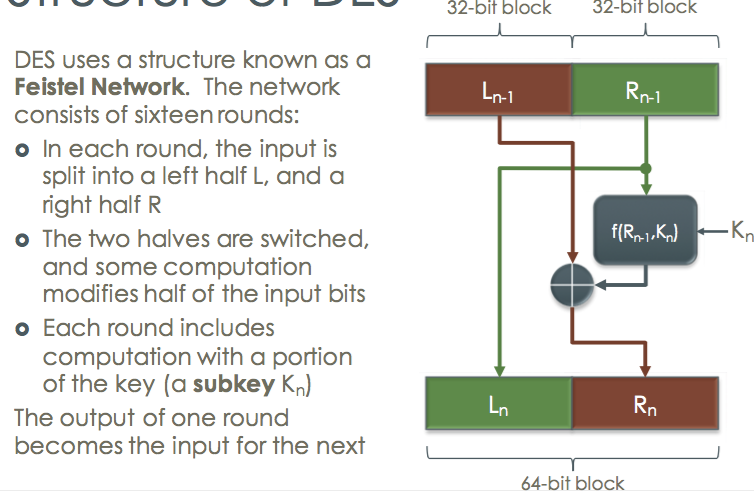
Block Cipher



Block Cipher Design:



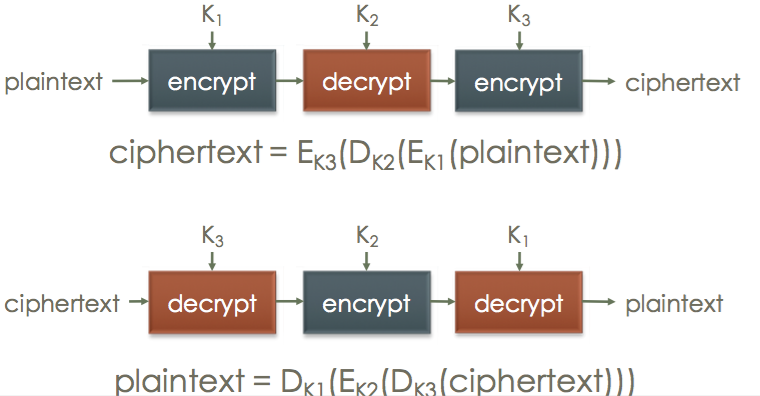
DES: Data Encryption Standard



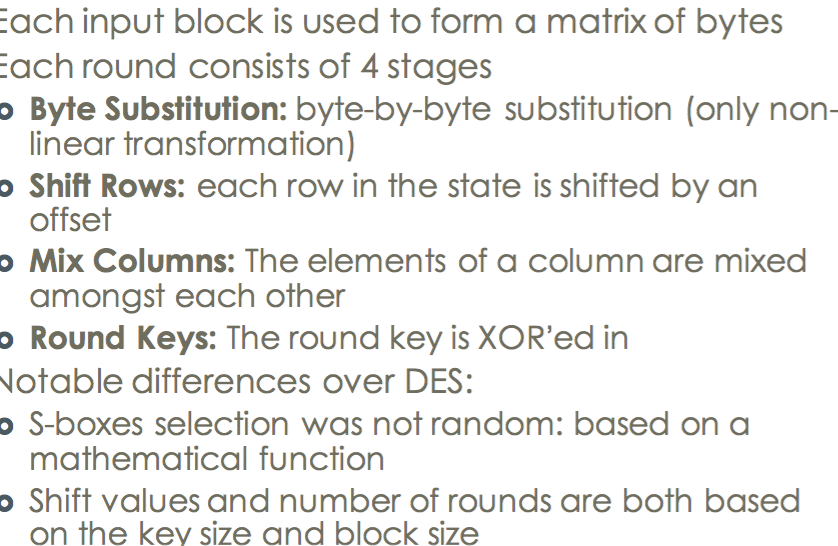
3DES

splitting a 168-bit key into three 56- bit parts

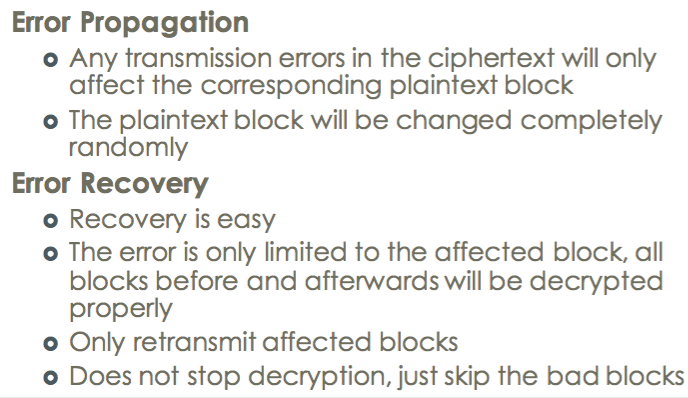
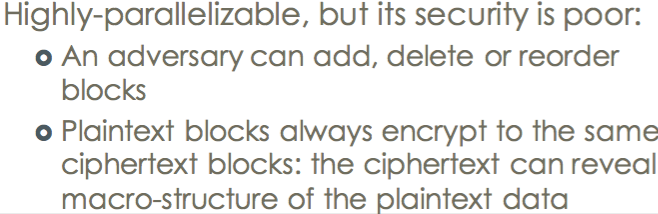
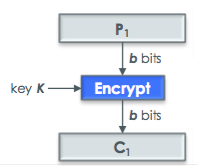
and running the algorithm three times

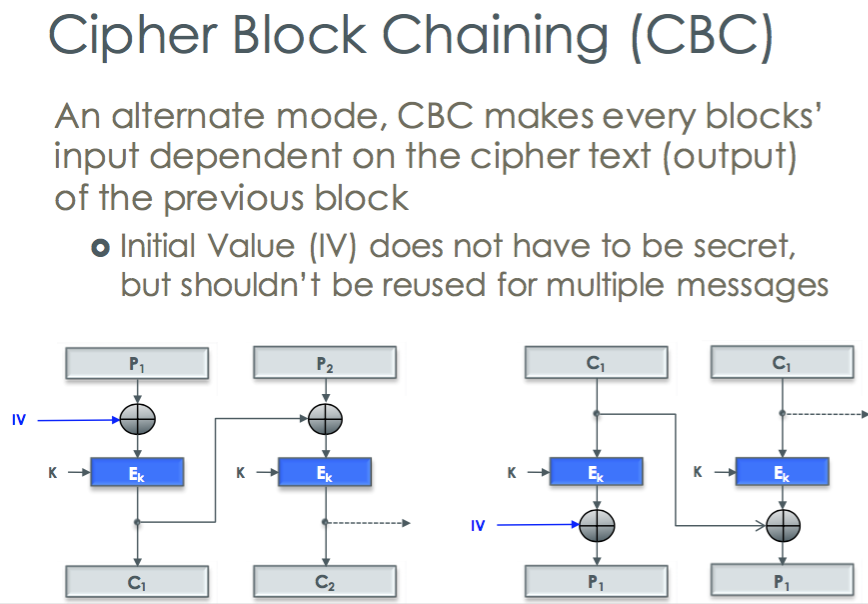


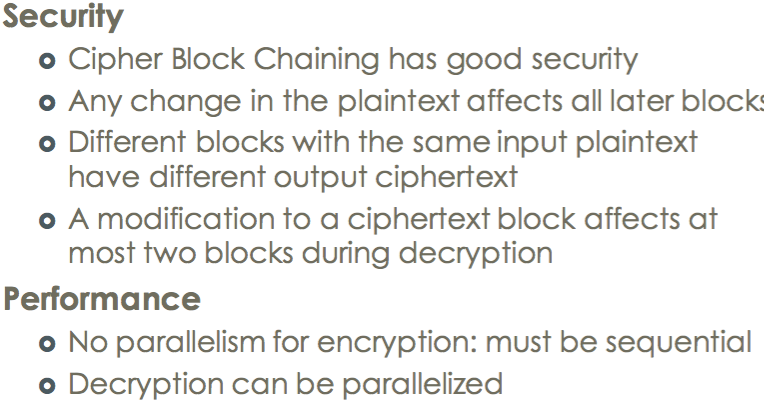
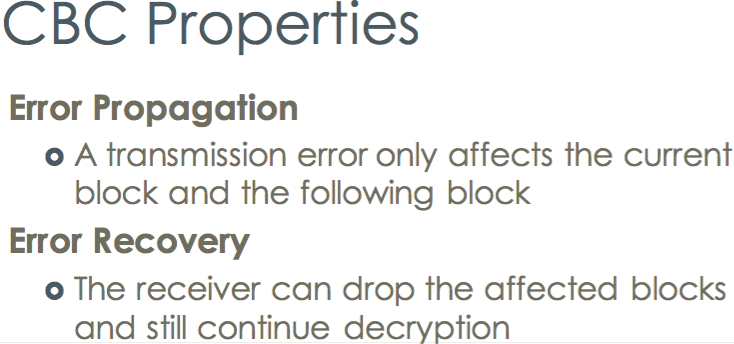
AES



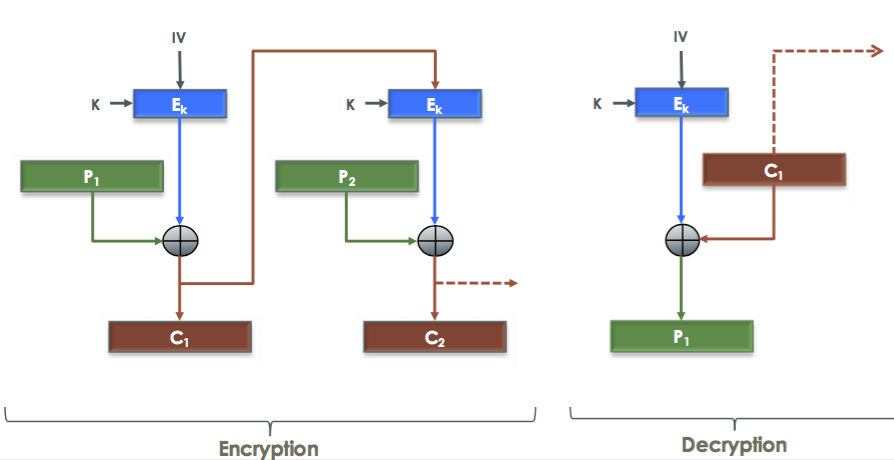
ECB Electronic Codebook



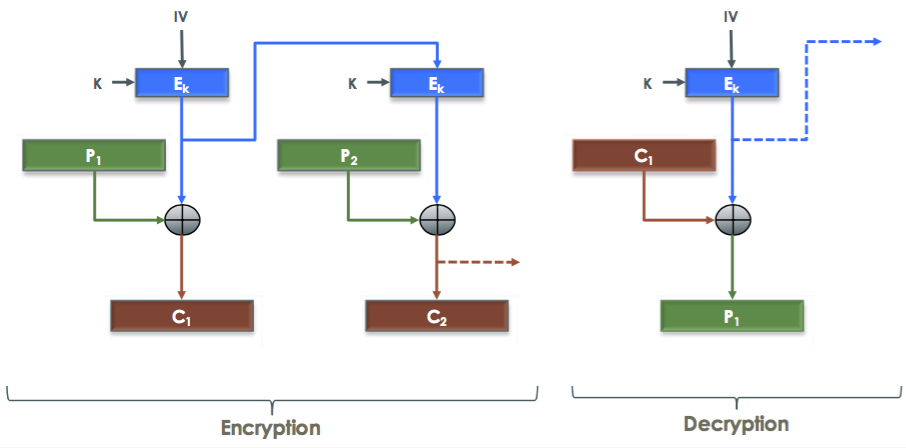
Cipher Block chaining (CBC)

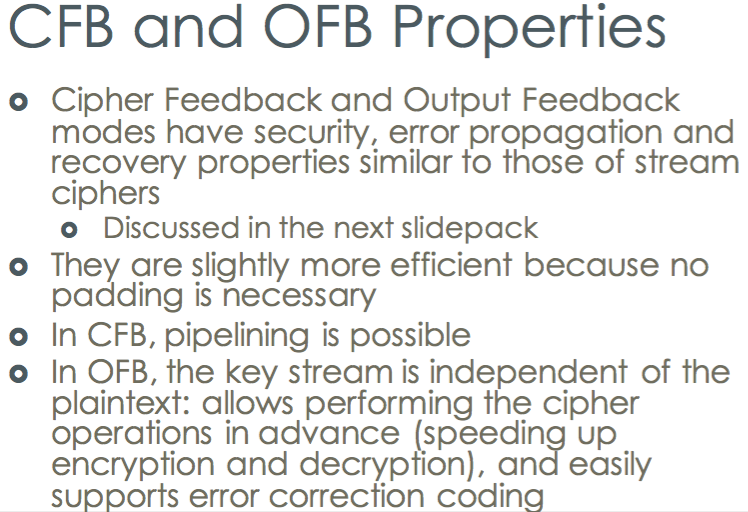


Cipher Feedback (CFB)

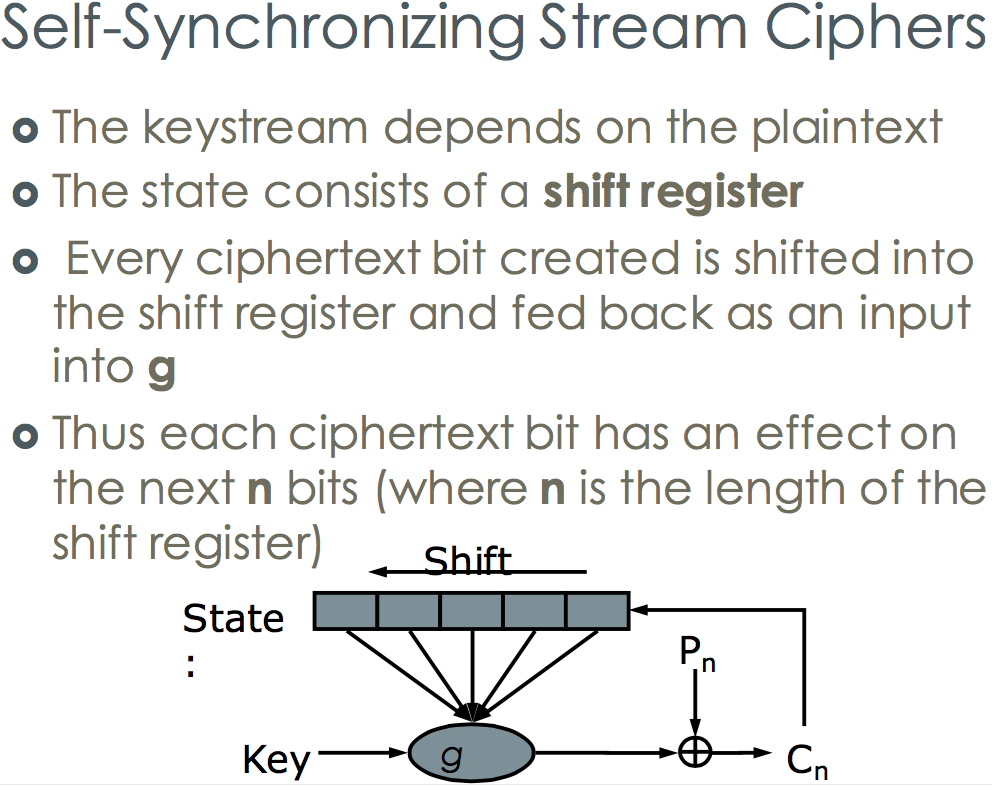
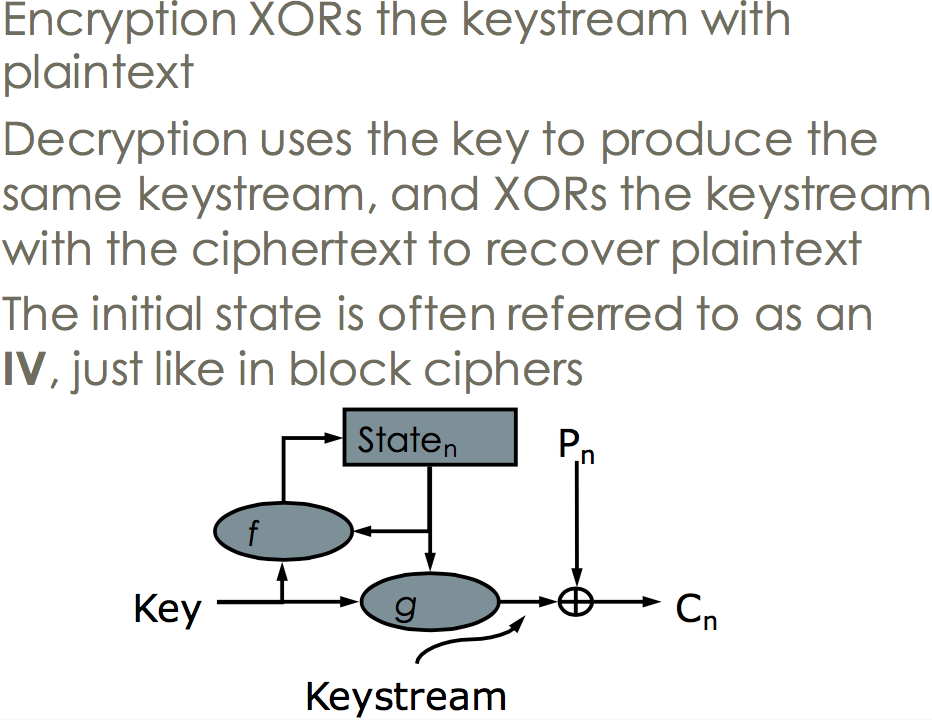


Output Feedback (OFB)

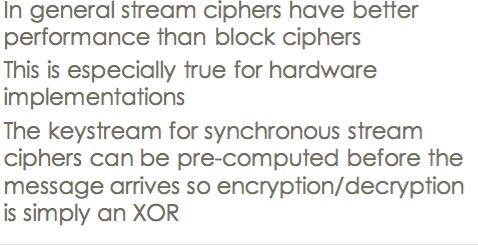
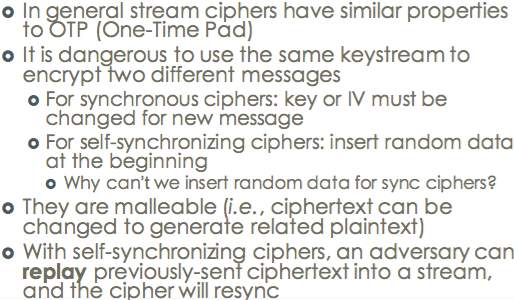




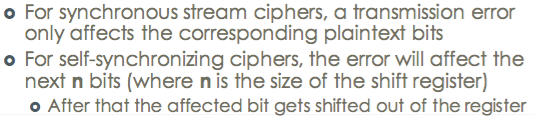
Stream cipher

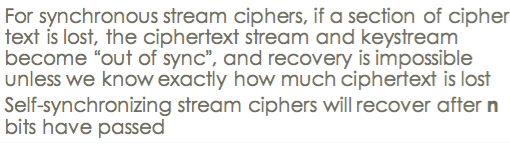


Security && Performance

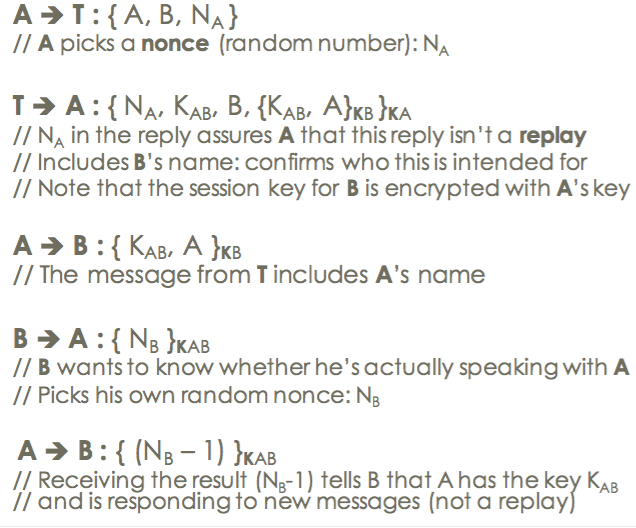


Error propagation && Error Recovery

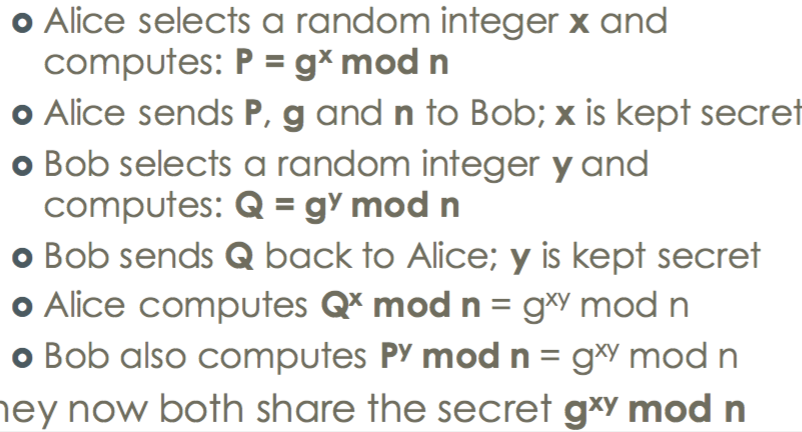




Needham-Schroeder Protocol



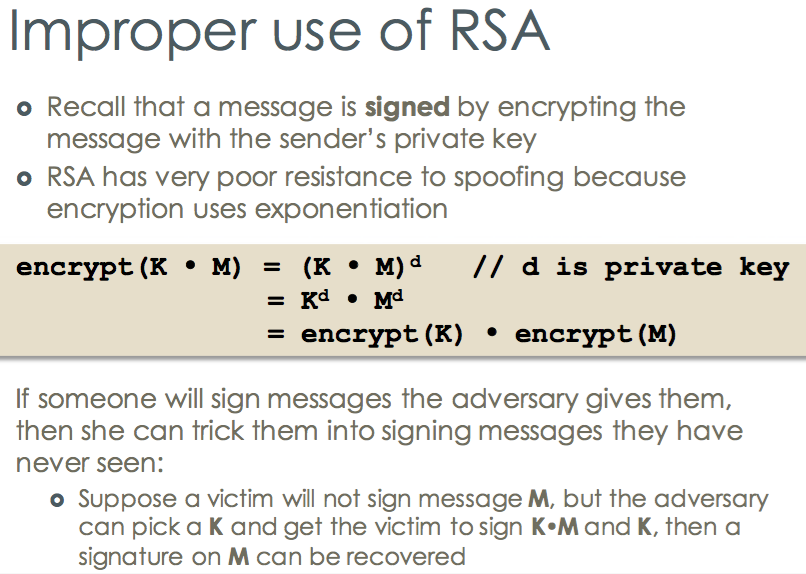
Diffie-Hellman Key Exchange



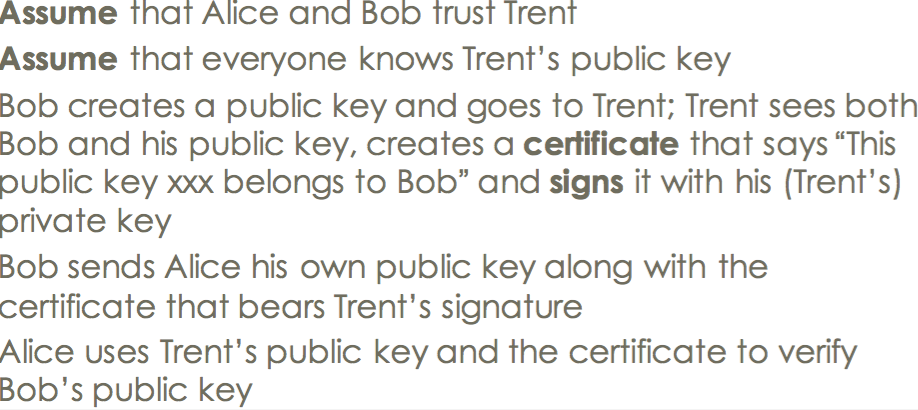
Public Key Encryption

the sender encrypts the message with the intended recipient’s public key, Only the recipient should have the private key, so only the recipient can decrypt the message

Public Key Authentication

For authentication, the message is encrypted with the sender’s private key (also called signing), Any recipient can decrypt using sender’s public key, Only sender could have encrypted the text we received, thus providing authentication and non-repudiation

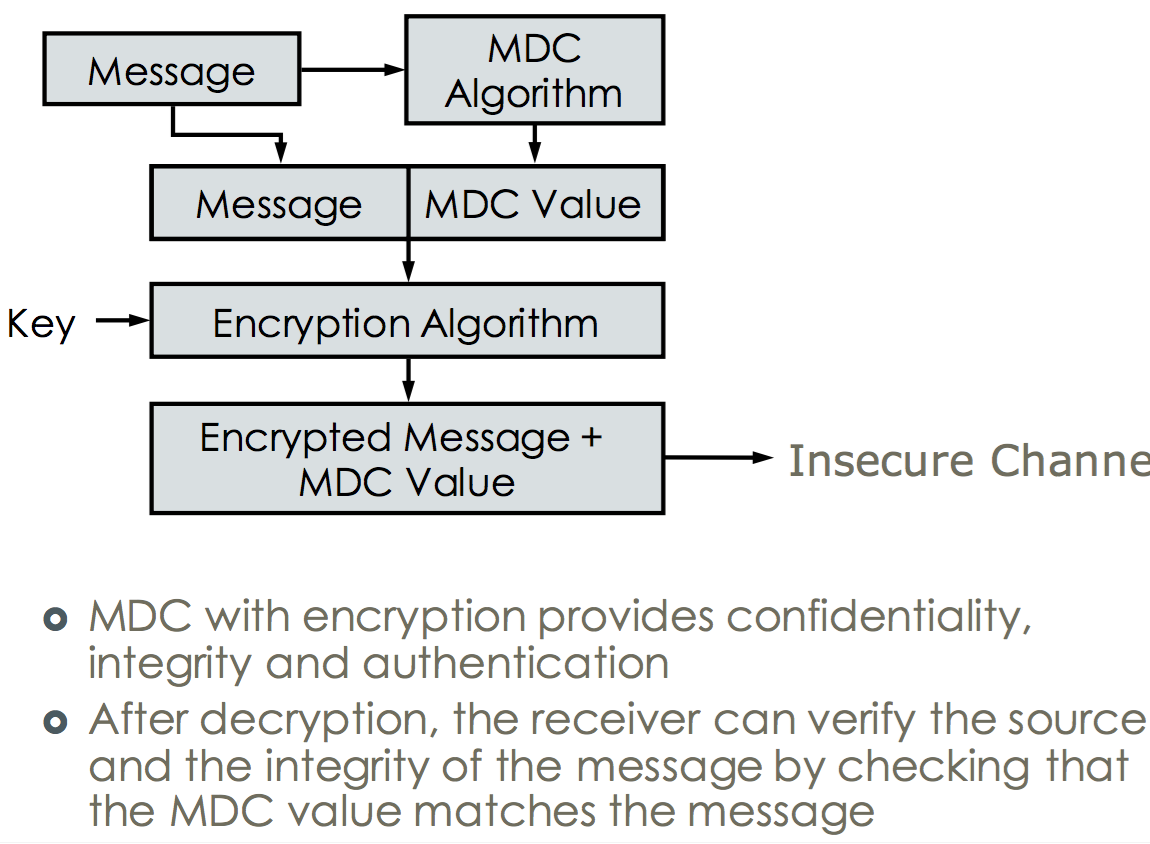
Public key Cryptography



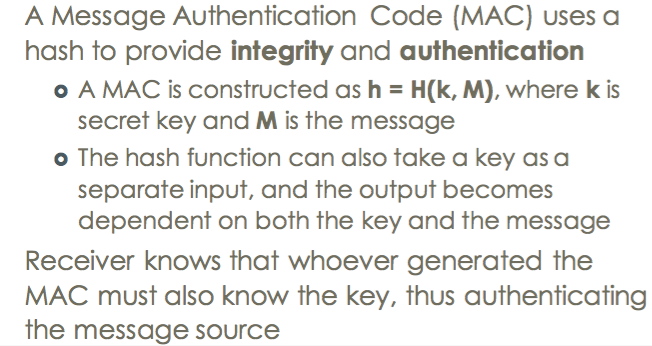
PGP: An Alternative to PKI

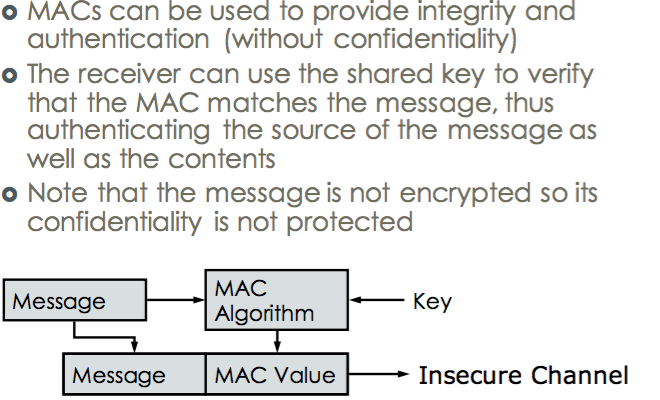
Public key exchange

Modification Detection Code -> Using MDC

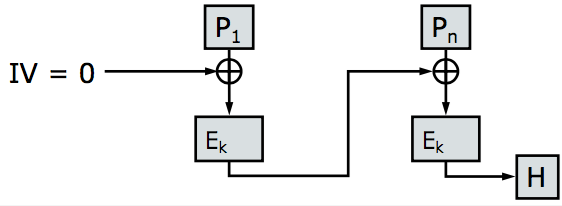


Message Authentication Code





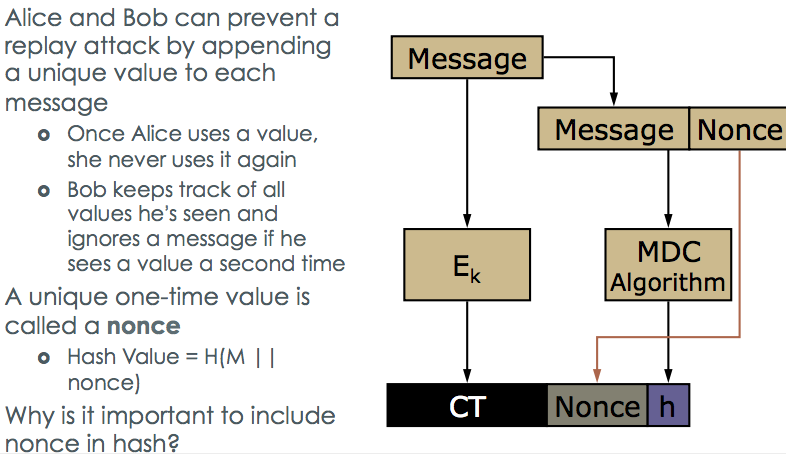
MAC using Symmetric Ciphers CBC-MAC



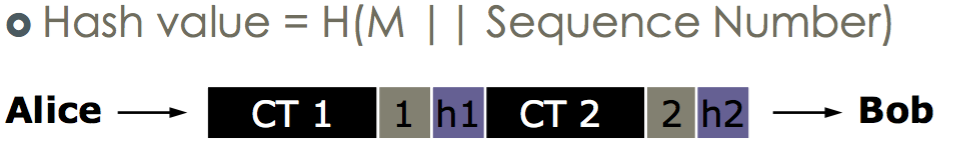
MAC using Hashes

HMAC = H[(K ⊕ opad) || H((K ⊕ ipad) || M)]

Replay attack



Reorder attack



SSL

