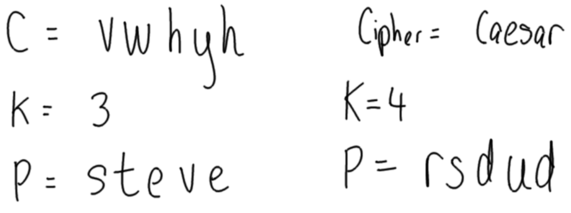
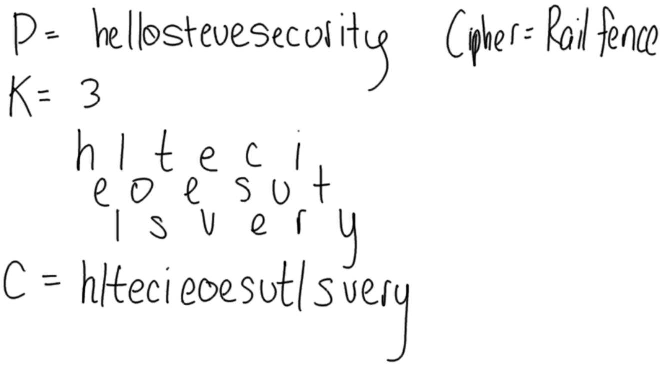
ITS335 – Cryptography Notes



C = vwhyh
K = 3
P = steve

Cipher = Caesar
K=4
P= rsdud

Figure 1: Substitution cipher example; Lecture 02



P= hellostevesecurity
Cipher= Rail fence
K= 3

h l t e c i
e o e s u t
l s v e r y

C = hltecieoesutlsvery

Figure 2: Transposition cipher example; Lecture 02

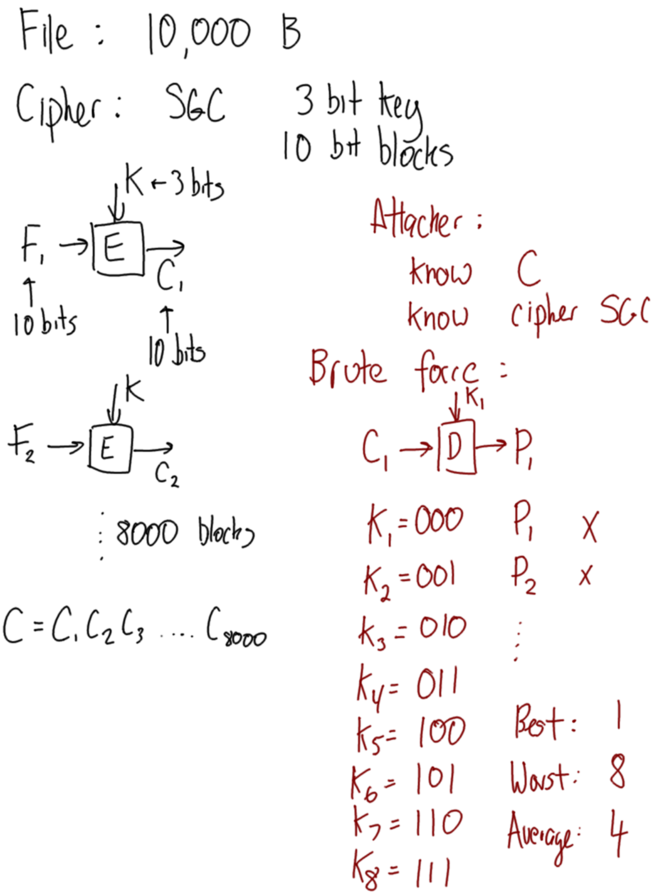
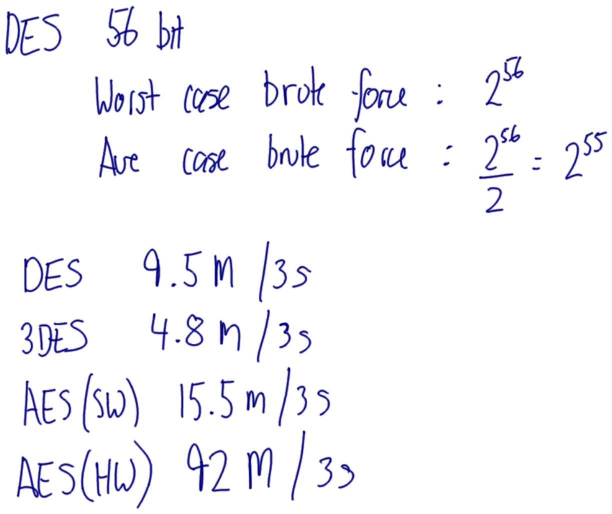


Figure 3: Concept of brute force attack; Lecture 03



DES 56 bit

Worst case brute force : 2^{56}

Ave case brute force : $\frac{2^{56}}{2} = 2^{55}$

DES	9.5 M / 3 s
3DES	4.8 M / 3 s
AES (SW)	15.5 M / 3 s
AES (HW)	92 M / 3 s

Figure 4: Brute force on DES and speeds; Lecture 03

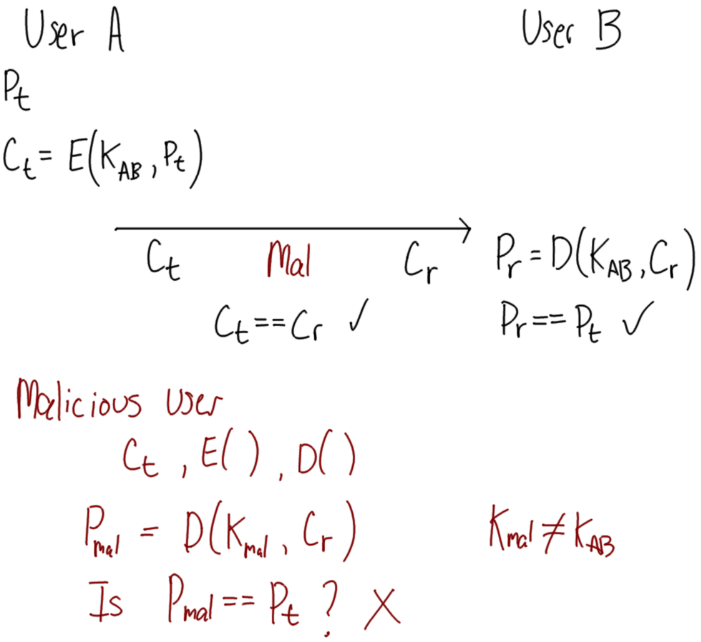


Figure 5: Confidentiality with Encryption and Attack; Lecture 04

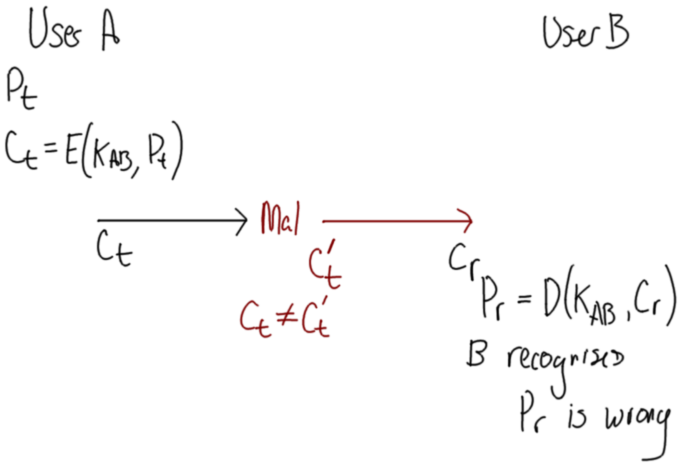


Figure 6: Data Integrity with Encryption and Attack 1; Lecture 04

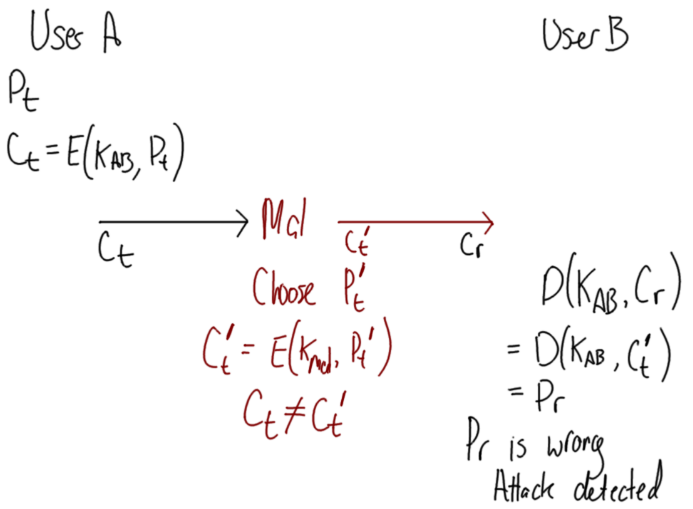


Figure 7: Data Integrity with Encryption and Attack 2; Lecture 04

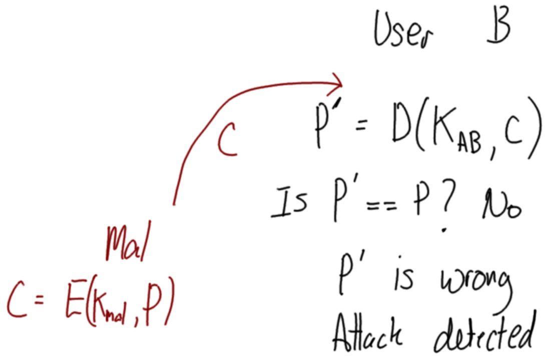


Figure 8: Source Authentication with Encryption and Attack; Lecture 04

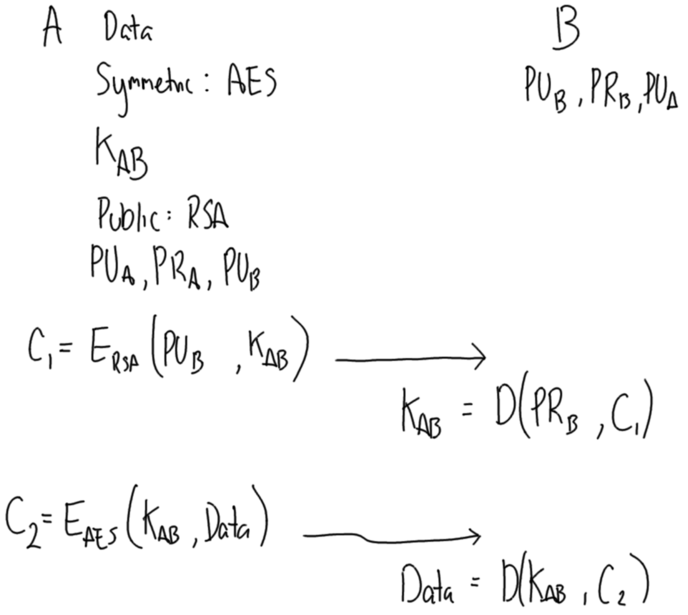


Figure 9: Public Key Crypto and Symmetric Key Crypto; Lecture 05