Jan 24, 2005 -- Lecture 3

22C:169
Computer Security

Douglas W. Jones

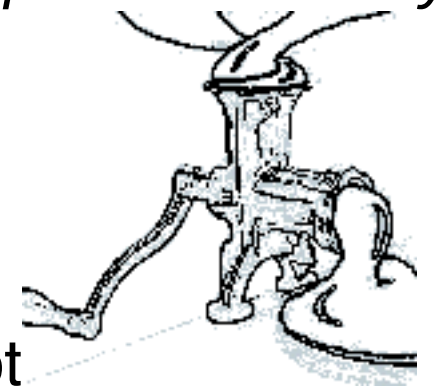
Department of Computer Science

Cryptography

Encryption (Encoding)

cleartext

plaintext *encryption key*

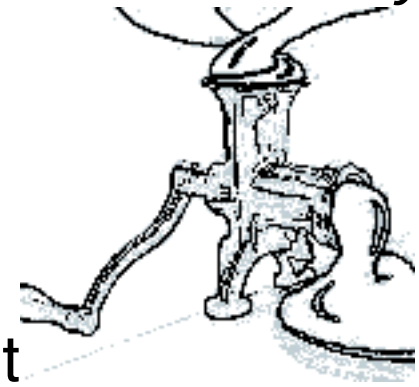


encrypt *cyphertext*

$cyphertext = F_{encrypt}(plaintext, key_{encrypt})$

Decryption (Decoding)

cyphertext *decryption key*



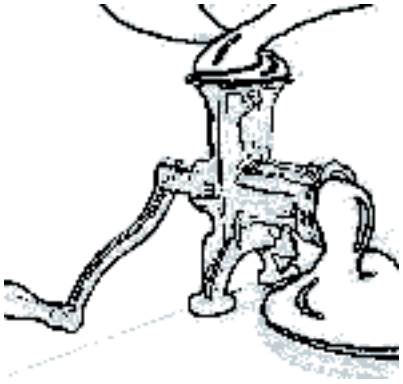
decrypt *plaintext*

$plaintext = F_{decrypt}(cyphertext, key_{decrypt})$

$t = F_{decrypt}(F_{encrypt}(t, k_{encrypt}), k_{decrypt})$

Cryptanalysis or Code Breaking

cyphertext *contextual knowledge*



crack *decryption key*

$k_{decrypt} = F_{crack}(cyphertext)$

In an Ideal world, we hope for

for a message of length n

$F_{encrypt} = O(n)$

$F_{decrypt} = O(n)$

F_{crack} *not in* computable

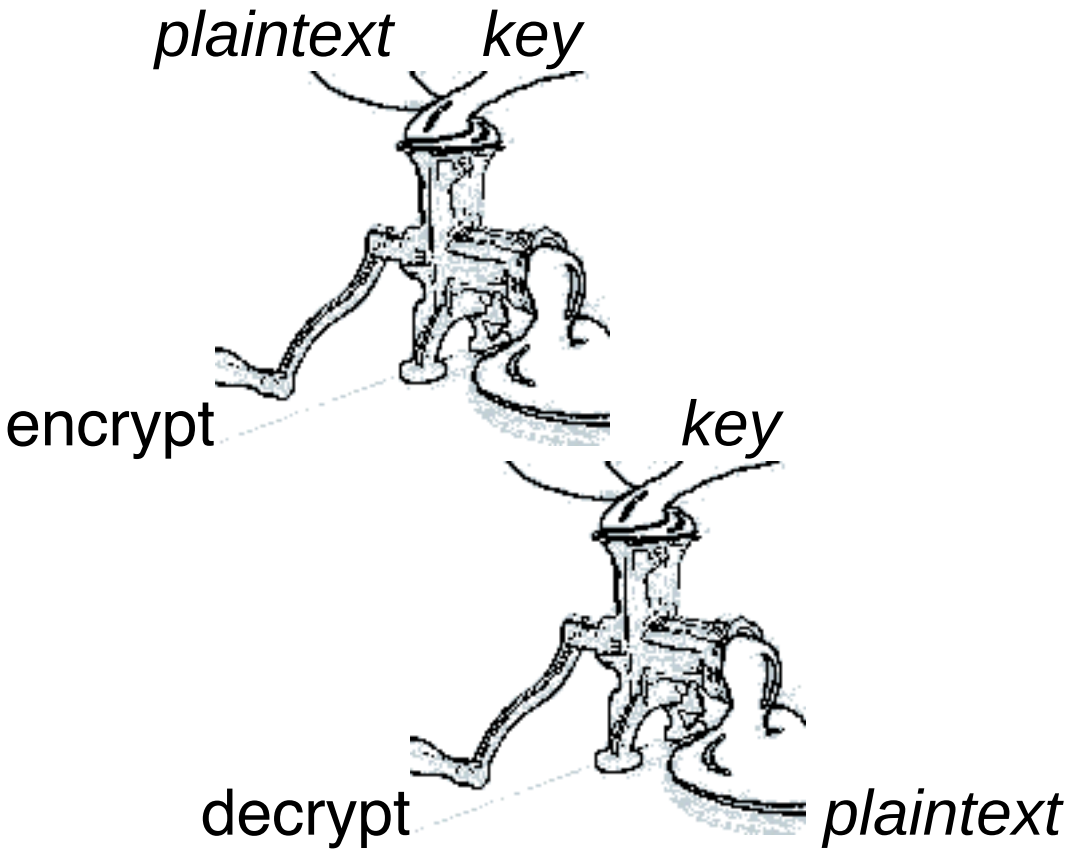
In the real world, we might accept

$F_{encrypt}$ *in* P

$F_{decrypt}$ *in* P

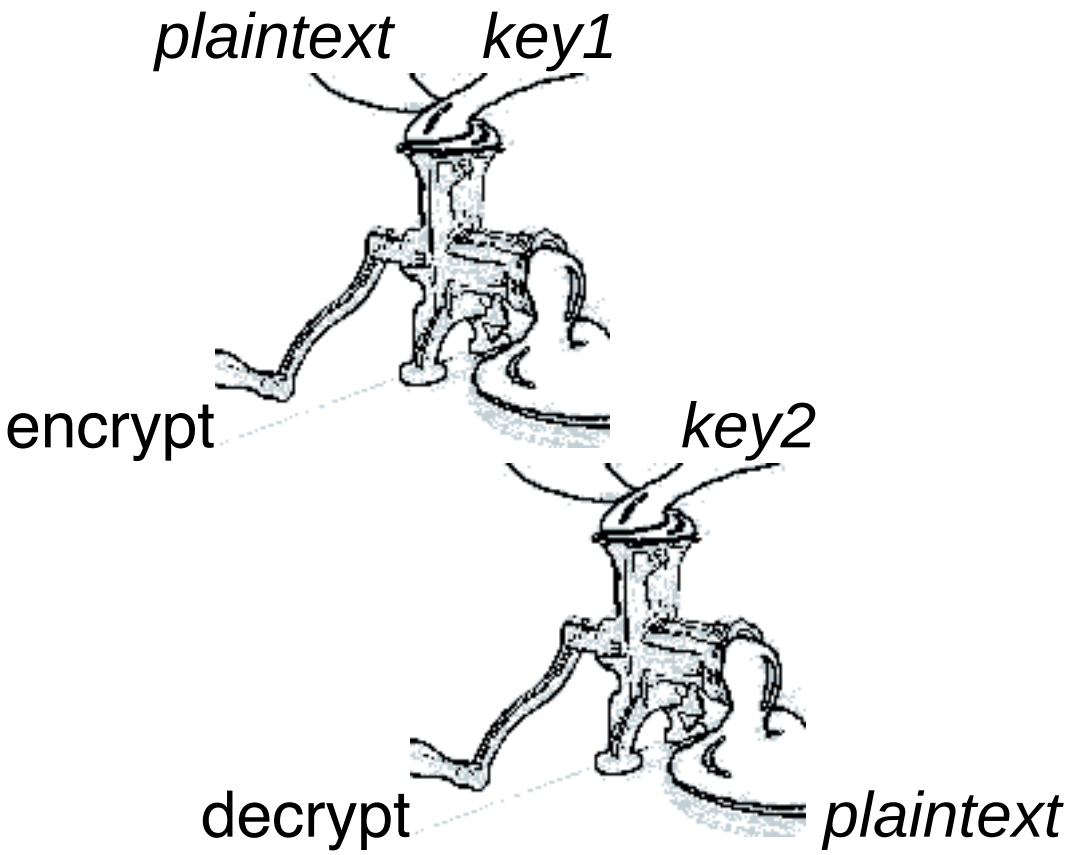
F_{crack} *in* NP

Symmetric Key Cyphers



$$t = F_{\text{decrypt}}(F_{\text{encrypt}}(t,k),\ k)$$

Public Key Cyphers



$t = F_{\text{decrypt}}(F_{\text{encrypt}}(t,k_1),\ k_2)$

$<k_1,k_2> = F_{\text{key generate}}(k_{\text{master}})$

Example: Julius Caesar's Cypher

plaintext = "Veni Vidi Vici"

$F_{encrypt}$ = for each character, add k

$F_{encrypt}$(*plaintext*, 4) = "Zirm Zmhm Zmgm"

$F_{decrypt}$ = for each character, subtract k

for k = 13 on a 26 letter alphabet,

$F_{encrypt} = F_{decrypt}$

Caesar Cypher = simple letter substitution

Captain Midnight Decoder Ring

1940-41

Example: Exclusive Or Cyphers

$F_{encrypt}(t, k) = t \oplus k$

$F_{decrypt}(t, k) = t \oplus k$

plaintext = `10001011111000`
k = `10100101100001`
cyphertext = `00101110011001`

So long as keys are
random and never reused
this code cannot be broken!