AES & DES encryption stds.

Today's lecture: Advanced encryption std.
Data encryption std.

DES First, most studied cipher in world

1974 by IBM + NSA [redacted]

Faithfully worked

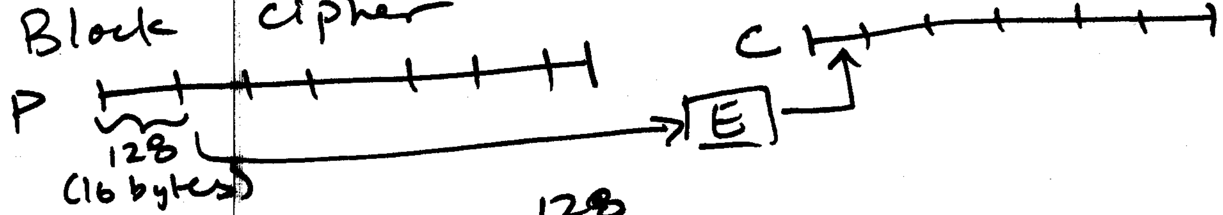
Issues: ① Small key size (3) 97 - RSA Challenge
② poorly optimized (4) 99 - DES Cracker

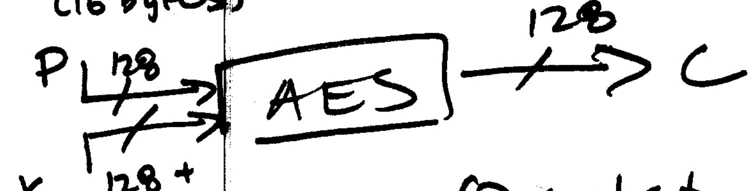
Except: 3DES, run 3 times in a row

AES

NIST competetion

Block cipher

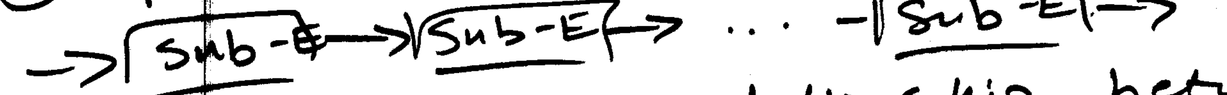




Major blocks: ① subst. ② transposition

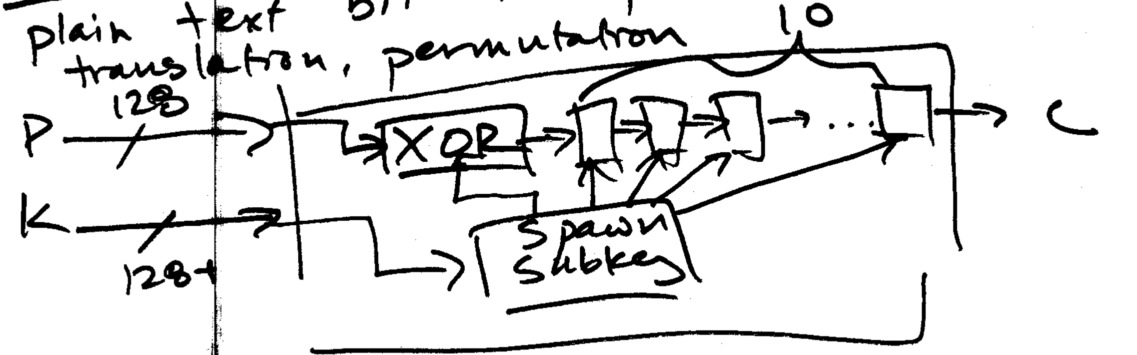
③ bitwise XOR
-Recall P XOR P=1 => (P XOR K) XOR K = P

④ repetition: iterate ciphers:

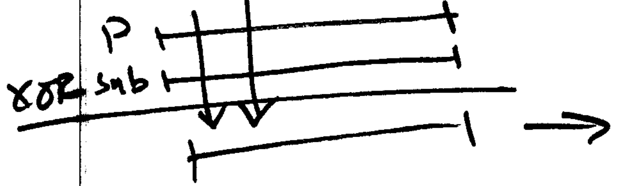


Shannon: Confusion: relationship between plain & cipher text is obscured, eg. subst.

diffusion: The influence of one or of each plain text bit is spread over many bits, eg. translation, permutation

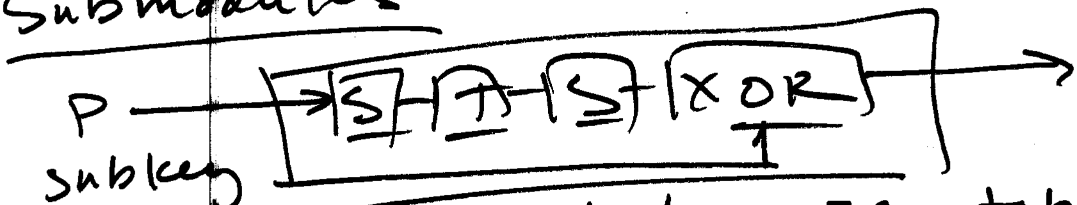


XOR



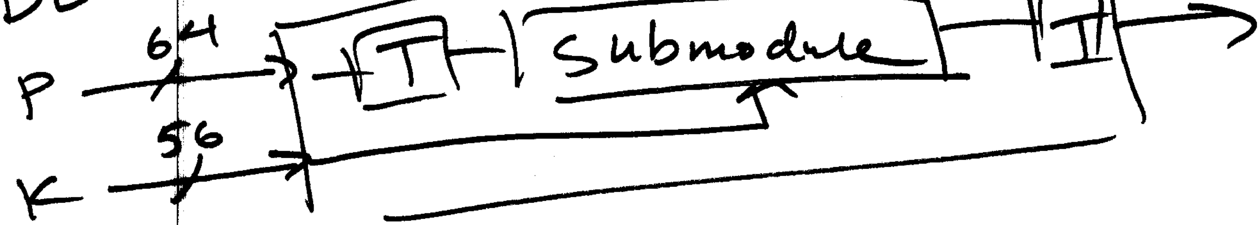
A	B	C
0	0	0
0	1	1
1	0	1
1	1	0

Submodules

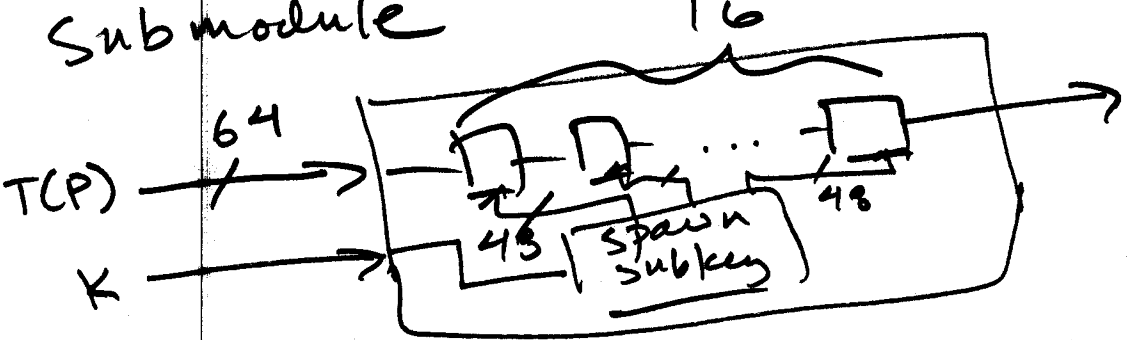


subsitution (S) : byte wise, table
transposition (T) : 4 byte, reorder, formula

DES



Submodule


16
64
T(P)
K
48
48
spawn subkey