ecs253 {PRIVATE }
April 16, 1997
Computer Security notes

DES - Data Encryption Standard (unbroken)

- main function: secrecy. Not used for classified data
- takes in 64 bits, outputs 64 bits, key is 56 bits (ignore parity bit)
- encipher and decipher blocks of data
- deciphering is the reverse processes of the enciphering processes

IDEA cipher - fixes weaknesses in DES
Lucifer Cipher - key changed from 128 to 64 bits. Good cipher
Product cipher - uses transposition and substitution at the bit level. Is also a round cipher (iterates 16 times, 16 different keys).

DES - 3 parts
1) Initial Permutation (IP) (*see page 17 of the Data Encryption Standard Handout*)
- Used to generate 16 sets of keys ("round keys") used to encipher

2) Complex key-dependent computation (*see page 8 of the Data Encryption Standard Handout* )
- defined in terms of function f (the cipher function) and KS (the key schedule)
- strength lies in how hard it is to invert f.
(*see page 11 of the Data Encryption Standard Handout*)

3) Inverse Initial Permutation ($IP^{-1}$)

Things people noticed:

1) Complementation Problem (Diffie & Hellman):
$DES_k(M) = C$ $DES_e(M') = C'$

2) Certain keys contain their own inverses
$DES_0(M) = C$ $DES_0(C) = M$

3) Double Encipherment does not help.
if $(DES_{k2}(DES_{k1}(M)) = C$ then
$DES_{k3}(M) = C$

How good is key length?

4) Differential Cryptanalysis
focus on plaintext and ciphertext pairs

C1 xor C2 = b

M1 xor M2 = b'

DES modes:
1) ECD - straight DES. On it's way to being broken.
2) CBC - Cipher Block Chain
3) Triple DES - uses only 3 keys
4) EDE mode - uses 2 keys to add more complexity
$(DES_{k1}(DES^{-1}_{k2}(DES_{k1}(M)))$

Public Key Cryptography (Diffie and Hellman):
- Created key exchange protocol
- How do you distribute keys?
- use 2 keys: 1) public - available to all ( E )
2) private - you are the only one who knows it (D)

RSA - an exponentiation cipher
C, M elem [0, n - 1]

$M^e \bmod n = C$
$C^d \bmod n = M$

in order for this to work:
1) $(M^e \bmod n)^d \bmod n = M$ or
2) $M^{ed} \bmod n = M$
must hold

$ed \bmod g(n) = 1$
$M^{ed} \bmod n = M^{1+kg(n)} \bmod n$
( $ed \bmod g(n) = 1 <=> ed = 1 + k\, g(n)$ )
$= M (M^{g(n)})^k \bmod n$
$= M (M^{g(n)} \bmod n)^k \bmod n$
$= M ( 1 ) \bmod n$

pick two large primes, p & q
$p * q = n$

pick e so that this holds:
$ed \bmod g(n) = 1$
where
$g(n) = (p - 1)(q - 1)$

d is a private key and the pair of e & n are public

take message, M
$M^e \bmod n = C$
$e^d \bmod n = M$ (to decipher)

example:
$p = 5, q = 7, => n = 35, g(n) = 24$

e = 11
$11^d \bmod 24 = 1$, so d = 1

M = hello ( message must not exceed 25 )

so, h e l l o
maps to 07 04 11 11 14

use $28^{11} \bmod 37 = 7$ to decipher

Note: *g(n)* -> since e and n are unknown, it is easy to break the cipher. However, n cannot be factored and you can't break the cipher.