Lecture 5: DES Use and Analysis

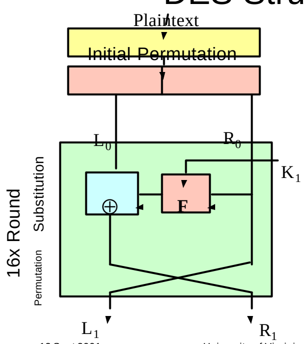
CS588: Security and Privacy
University of Virginia
Computer Science

David Evans
http://www.cs.virginia.edu/~evans

Menu

- Today's manifest: on line only
- DES Review
- Modes of Operation
- 3DES
- DES Attacks
- Return PS1

DES Structure

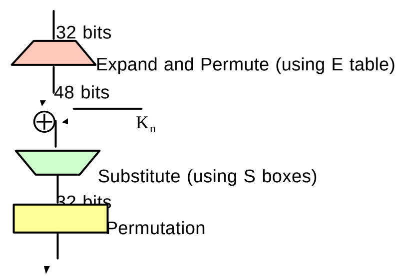


L_0 = left half of plaintext
R_0 = right half of plaintext

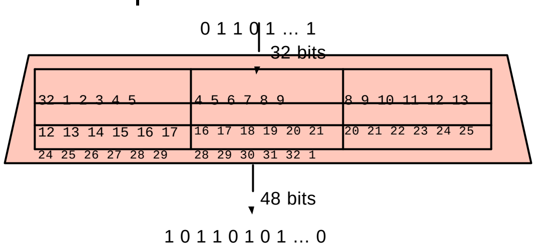
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

$C = R_n \| L_n$
n is number of rounds
(undo last permutation)

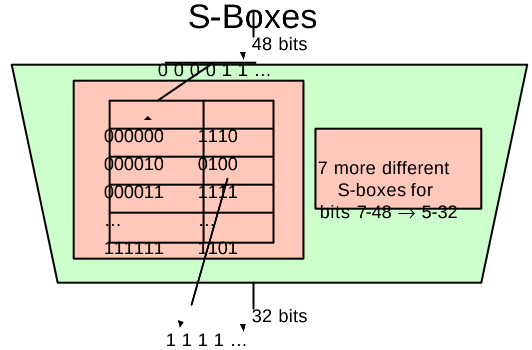
DES's F



Expansion/Permutation



S-Boxes



Nothing secret about the S-Boxes (but they are confusing)

Modes of Operation

Modes of Operation

- Transmitting a long plaintext using DES:

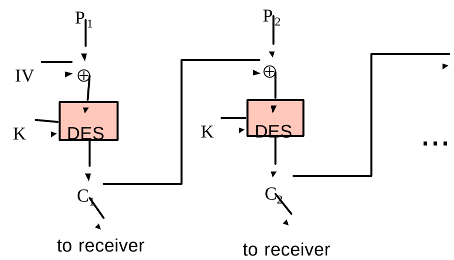
  $P = P_1 \| P_2 \| \ldots \| P_N$

- Electronic Codebook Mode:

  $C = E_K(P_1) \| E_K(P_2) \| \ldots \| E_K(P_N)$

- Problems:
  - Any identical blocks encrypted identically
    - 64 bits = 8 ASCII characters
  - Lots of ciphertext encrypted with same K

Cipher Block Chaining



Cipher Block Chaining

$C_i = E_K(P_i \oplus C_{i-1}) \qquad C_1 = E_K(P_1 \oplus IV)$

Decrypt:

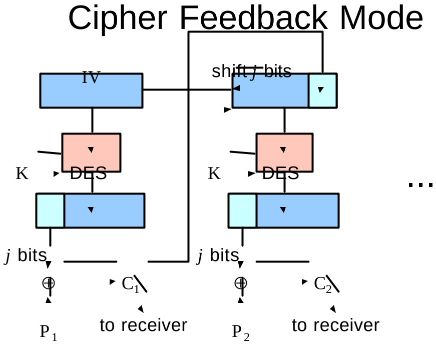
$M_i = D_K(C_i) \oplus C_{i-1}$

$M_1 = D_K(C_1) \oplus IV$

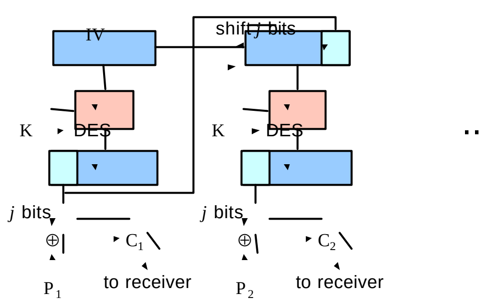
$D_K(E_K(P_i \oplus C_{i-1})) \oplus C_{i-1}$

$= P_i \oplus C_{i-1} \oplus C_{i-1} = P_i$

Cipher Feedback Mode



Output Feedback Mode



Cipher/Output Feedback

- 1-bit transmission error
- Active eavesdropper
- Performance

Multiple Encryption

Multiple Encryption

- $C = E_{K2} (E_{K1} (P))$
- Does it double the key space?
- Monoalphabetic cipher

$$C_i = K_2[K_1[P_i]]$$
$$= K_3[P_i] \text{ for some } K_3$$

Double-Vigenère

$C = E_{K2} (E_{K1} (P))$

Vigenère: $C_i = (P_i + K_{i \bmod N}) \bmod Z$

$C_i = ((P_i + K1_{i \bmod N1} \bmod Z) + K2_{i \bmod N2}) \bmod Z$

$= (P_i + K1_{i \bmod N1} + K2_{i \bmod N2}) \bmod Z$

if $N1 = N2$:

$= (P_i + K3_{i \bmod N}) \bmod Z \quad (K3 = K1 + K2)$

what if $N1 \neq N2$?

Double-Vigenère

- K1 = "BOND"
- K2 = "JAMES"

```
  BONDBONDBONDBONDBONDBONDBOND
+ JAMESJAMESJAMESJAMESJAMESJAM
= KOZHTXNPFGWDNSFMBARVKOZHTXNP
```

- Effective key length: LCM (N1, N2) = 20

Double DES

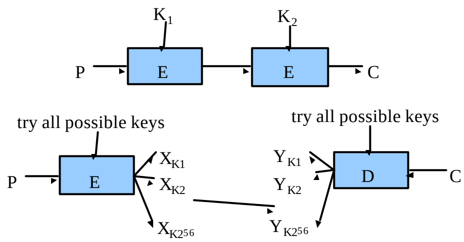
- $C = E_{K2} (E_{K1} (P))$
- Is there a K3 such that $C = E_{K3} (P)$?
  - There are 2^{56} keys, and $2^{64}!$ mappings
  - If DES is good, keys map randomly to mappings.
  - Probability that a randomly chosen mapping corresponds to a DES key:

    $2^{56} / 2^{64}! << 1 / 2^{63}!$
- Effective key size of Double DES?

  $= 2^{56} * 2^{56} = 2^{112}$

  WRONG!

Known Plaintext Attack



One $X_{Ki} = Y_{Kj}$ means $K_1 = K_i$ and $K_2 = K_j$

Meet-in-the-Middle Attack

- $C = E_{K2}(E_{K1}(P))$
- $X = E_{K1}(P) = D_{K2}(C)$
- Brute force attack (given one P/C pair):
  calculate $E_{K1}(P)$ for all keys (2^{56} work)
  calculate $D_{K2}(C)$ for all keys (2^{56} work)
  the match gives the keys
- Total work = $2 * 2^{56} = 2^{57}$

2-Key Triple DES

- $C = E_{K1}(D_{K2}(E_{K1}(P)))$
- Why D_{K2} not E_{K2}?
  - Backwards compatibility with DES
  - If K1 = K2: $C = E_{K1}(D_{K1}(E_{K1}(P))) = E_{K1}(P)$
- Actual key size = 56 + 56 bits = 112 bits
- Meet-in-the-middle?
  - $X = E_{K1}(P) = D_{K1}(E_{K2}(C))$
    2^{56} need to try 2^{112}

How secure is Triple-DES

- Brute force search: 2^{112} keys
  - Best DES attack: 245 B keys/second
  - $\approx 6.7 * 10^{14}$ years (compared to 22 hours)
  - 10^{11} years = total lifetime of universe (closed universe theory)
- Best known attack - reduces to $2^{120-\log_2 n}$
  - n = number of known P-C pairs
  - n = 2^{64}, work is 2^{56}

Realistic?

3-Key Triple DES

- $C = E_{K3}(D_{K2}(E_{K1}(P)))$
- H(K) = 168
- Used by PGP, S/MIME
- How much work to brute-force?
  - Meet-in-the-middle:
    $X = D_{K3}(C) = D_{K2}(E_{K1}(P))$
    $2^{56} + 2^{112}$

DES Attacks

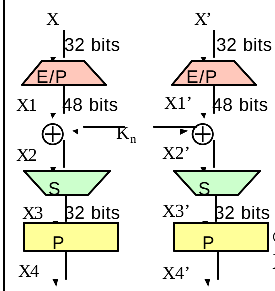
- Last time: brute force
  - Best result: 22 hours
  - But no where near good enough for 3DES
- Differential Cryptanalysis
- Power Cryptanalysis

Differential Cryptanalysis

- [Biham & Shamir, 1990]
- Choose plaintext pairs with fixed difference: $\Delta X = X \oplus X'$
- Use differences in resulting ciphertext to guess key probabilities
- With enough work (2^{47}) and enough chosen plaintexts (2^{47}) can find key (compared to 2^{56} brute force work)

Takes 3 years of 1.5Mbps encrypting chosen plaintext!

One Round

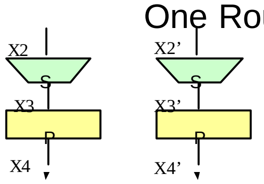


$\Delta X = X \oplus X'$
$\Delta X_i = 0$ iff $X_i = X_i'$

E/P preserves values:
$X_i = 0 \Rightarrow X1_{ep(i)} = X1_{ep(i)}'$
where ep(i) is a function defined by the E table

$\oplus$ preserves values:
$X2_i = X1_i \oplus K_n \quad X2_i' = X1_i' \oplus K_n$
$\Delta X_i = 0 \Rightarrow X2_{ep(i)} = X2_{ep(i)}'$

One Round, cont.



$\Delta X_i = 0 \Rightarrow X2_{ep(i)} = X2_{ep(i)}'$

$X3_i = X3_i' \Rightarrow X4_{p(i)} = X4_{p(i)}'$
(Known from ciphertext)

S-boxes are non-linear!
$\Delta X_i = 0 \not\Rightarrow X3_{s(ep(i))} = X3_{s(ep(i))}'$
But, maybe they do probabilistically:
$\Delta X_i = 0 \Rightarrow p(X3_{s(ep(i))} = X3_{s(ep(i))}') > .5$?
$p(X3_{s(ep(i))} = X3_{s(ep(i))}') < .5$?

Its a function of the key: p determined experimentally.

S-box: S1

6 bits: $x_1x_2x_3x_4x_5x_6$

$x_2x_3x_4x_5$ select column

x_1x_6	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
01	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
10	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
11	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

4 inputs to S1 produce 0: 011100, 000001, 111110, 111011

Partial pair XOR Distribution, S1

Input XOR / Output XOR

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	6	2	4	4	0	10	12	4	10	6	2	4
2	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
...																
3F	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

S-box: S1

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
01	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
10	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
11	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

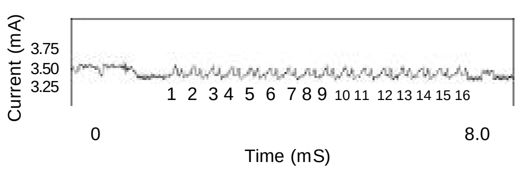
Difference in last input bit difference in output bits 0101
0001 + 0101 = 0100 (1 XOR 5 = 1)
1011 + 0101 = 1110 (B XOR 5 = E)

Differential Cryptanalysis

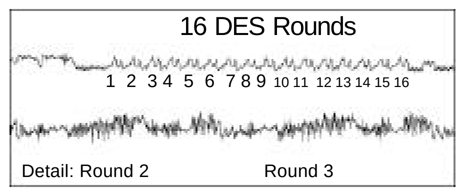
- Propagate experimental probabilities for 1 round through 16 rounds
- After enough P-C pairs, one key becomes most probable
- Difficulty depends heavily on S-Box choices
- First published in 1990, but NSA knew about it in 1973!

Differential Cryptanalysis

- "Successful" on DES up to 15 rounds (better than exhaustive search)
- By 16th round, characteristics probabilities are 2^{-56}
- Very successful on DES variants (breaks GDES with 6 chosen plaintexts)
- Very successful on FEAL (FEAL-4, FEAL-8, FEAL-N, FEAL-NX, ...)



DES Power Consumption



From http://www.cryptography.com/dpa/technical/index.html

Microprocessors use different amount of power depending on what they are doing!

Power Analysis Scenario

- Attacker has physical device that encrypts and decrypts using a secret key
- Is this realistic?

Smart Cards (Mondex)

Side Channel Cryptanalysis

- Regular Cryptanalysis: mathematical
  - Attacker sees inputs, outputs
- Side Channel Cryptanalysis
  - Attacker sees something else: power consumption, encryption/decryption time, radiation, etc.
- Depends on *implementation* of algorithm

Measuring Power Consumption

- Add a resistor between power source and device, measure voltage across resistor

  $I = V/R$
- Can sample at over 1GHz with < 1% error

Power Use Reveals Key

- Current for a left shift depends on leftmost bit:
  - if 1, need to set rightmost bit after
- DES key schedule uses shifts, can tell bits in key!
- Current for XOR may depend on number of switches

Defenses

- Reduce signal
  - Physical shielding, microprocessor design (make all shifts use same power, etc.)
- Introduce random noise
  - Change execution order, do random computation, etc.
- Design cryptosystems with DPA in mind
  - Nonlinear key updates between transactions

Charge

- Continue thinking about project ideas
  - Each project group should send me email or talk to me by next week about what you are considering
- Next time: modern block ciphers
  - Read AES papers before next class