Cryptanalysis

Lecture Block 3: Block Ciphers

John Manferdelli
jmanfer@microsoft.com
JohnManferdelli@hotmail.com

jlm20081013

Block ciphers

- Complicated keyed invertible functions constructed from iterated elementary rounds.
  - Confusion: non-linear functions (ROM lookup)
  - Diffusion: permute round output bits

Characteristics:

- *Fast*
- *Data encrypted in fixed “block sizes” (64,128,256 bit blocks are common).*
- *Key and message bits non-linearly mixed in cipher-text*

Mathematical view of block ciphers

- $E(k, x)=y$.
- $E: GF(2^m) \times GF(2^n) \longrightarrow GF(2^n)$, often $m=n$.
- $E(k,x)$ is a bijection in second variable.
- $E(k, x)$ in S_N, $N= 2^n$.
- Each bit position is a balanced boolean function.
- E is easy to compute but inverse function (with k fixed) is hard to compute without knowledge of k.
- Implicit function hard to compute.
- Intersection of algebraic varieties.

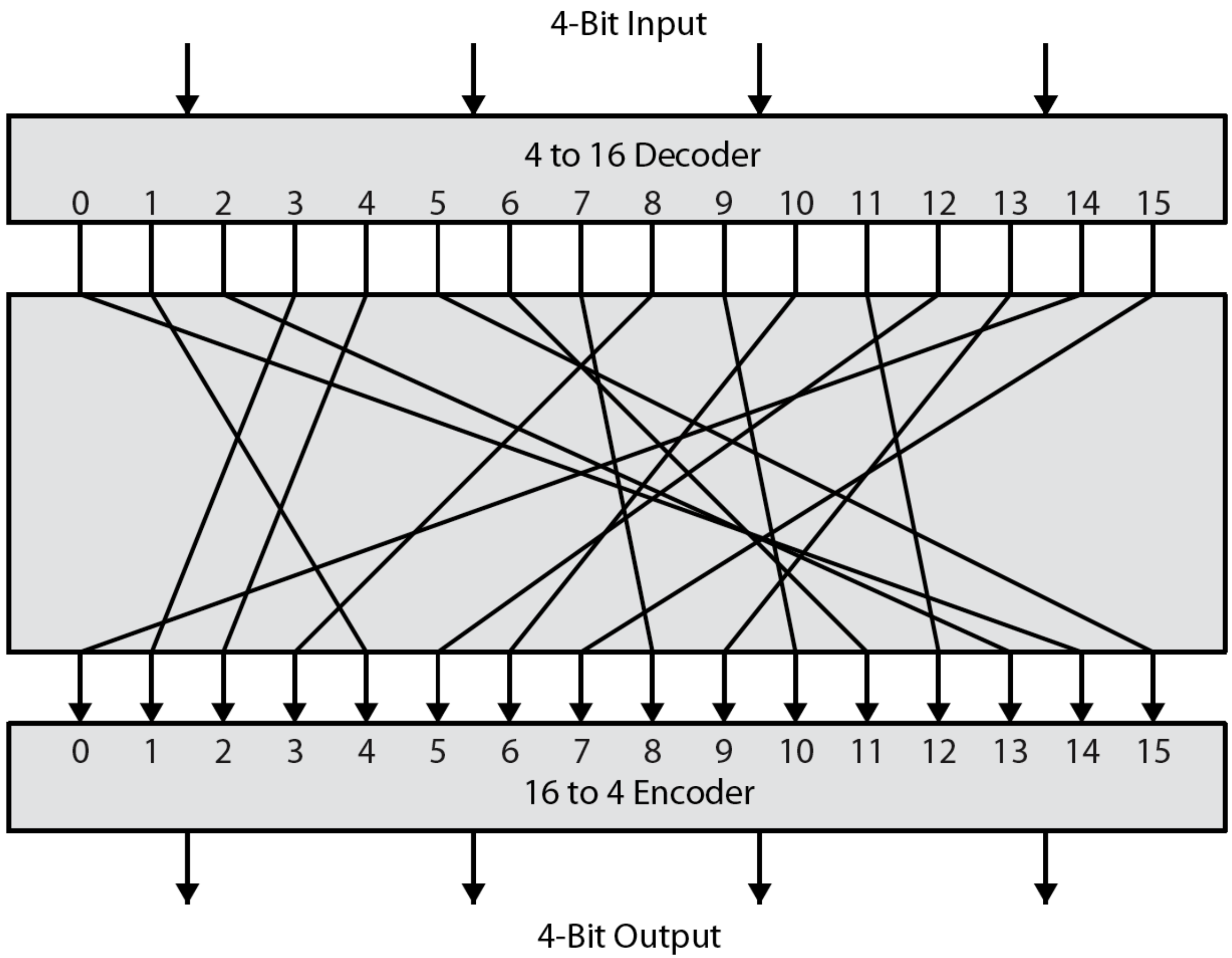
Guiding Theorems

- Implicit Function Theorem: If $F(x,y)= c$, is a continuously differentiable function from $R^n \times R^m$ into R^m and the mxm Jacobian in the y variables is non zero in a region, there is a function g from R^n to R^m such that $F(x, g(x))=c$. When F is linear, this function is very easy to compute. Think of g as mapping the plaintext to the key (for fixed ciphertext).

- Functions in over finite fields are polynomials: If f is a function from k^n to k, where k is a finite field, f can be written as a polynomial in the n variables.

- Reduction in dimension: Generally (pathological exceptions aside), if f is a function from k^n to k, where k is a finite field, and $f(x)=c$, one variable can be written as a function of the other n-1 variables. In other words, if g is a function from k^n to k subject to the constraint $f(x)=c$, then g can be rewritten as a function of n-1 variables.

What is a “safe” block cipher

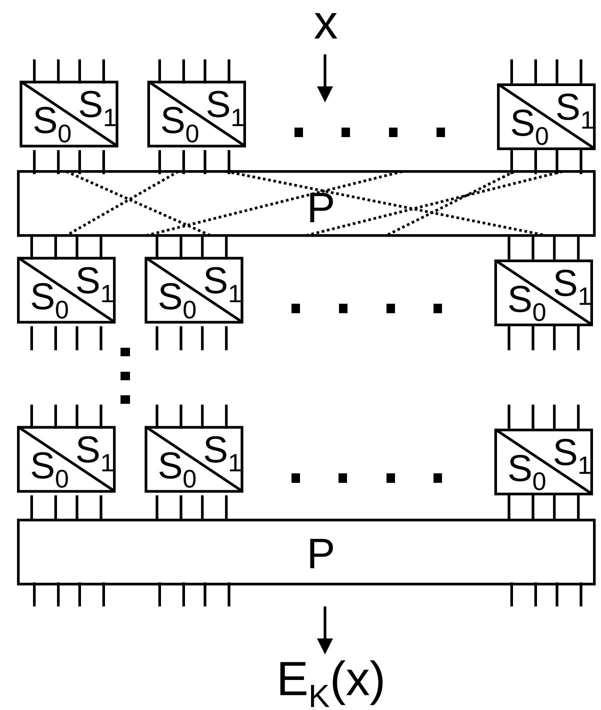


Data Encryption Standard

- Federal History
  - 1972 study.
  - RFP: 5/73, 8/74.
  - NSA: S-Box influence, key size reduction.
  - Published in Federal Register: 3/75.
  - FIPS 46: January, 1976.
- *DES*
  - Descendant of Feistel's Lucifer.
  - Designers: Horst Feistel, Walter Tuchman, Don Coppersmith, Alan Konheim, Edna Grossman, Bill Notz, Lynn Smith, and Bryant Tuckerman.
- Brute Force Cracking
  - EFS DES Cracker: $250K, 1998. 1,536 custom chips. Can brute force a DES key in days.
  - Deep Crack and distributed.net break a DES key in 22.25 hours.

Horst Feistel: Lucifer

- First serious needs for civilian encryption (in electronic banking), 1970's
- IBM's response: Lucifer, an iterated SP cipher
- Lucifer (v0):
  - Two fixed, 4x4 s-boxes, S_0 & S_1
  - A fixed permutation P
  - Key bits determine which s-box is to be used at each position
  - 8 x 64/4 = 128 key bits (for 64-bit block, 8 rounds)

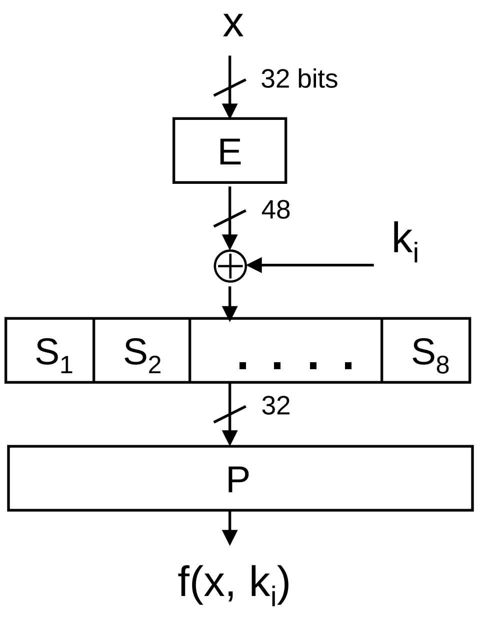


Graphic by cschen@cc.nctu.edu.tw

From Lucifer to DES

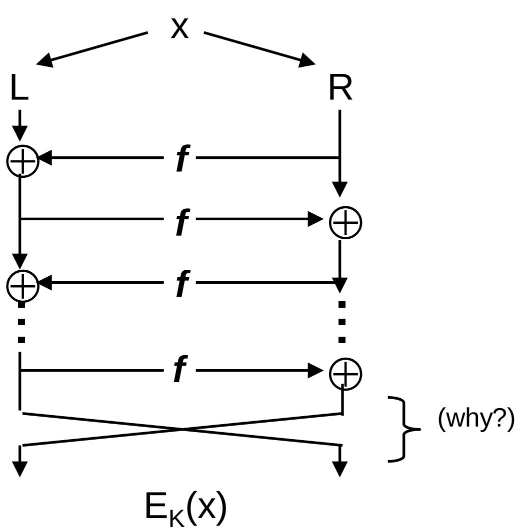
- 8 fixed, 6x4 s-boxes (non-invertible)
- Expansion, E, (simple duplication of 16 bits)
- Round keys are used only for xor with the input

- 56-bit key size
- 16 x 48 round key bits are selected from the 56-bit master key by the "key schedule".

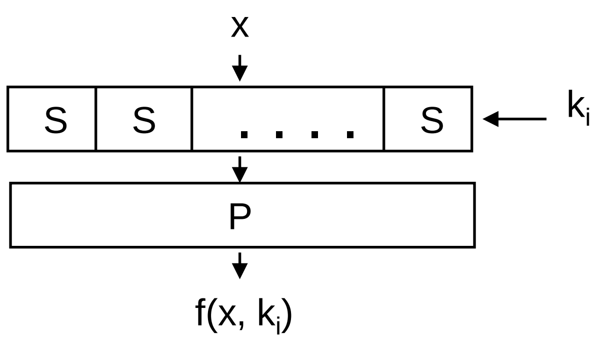


Feistel Ciphers

- A straightforward SP cipher needs twice the hardware: one for encryption (S, P), one for decryption (S^{-1}, P^{-1}).
- Feistel's solution:

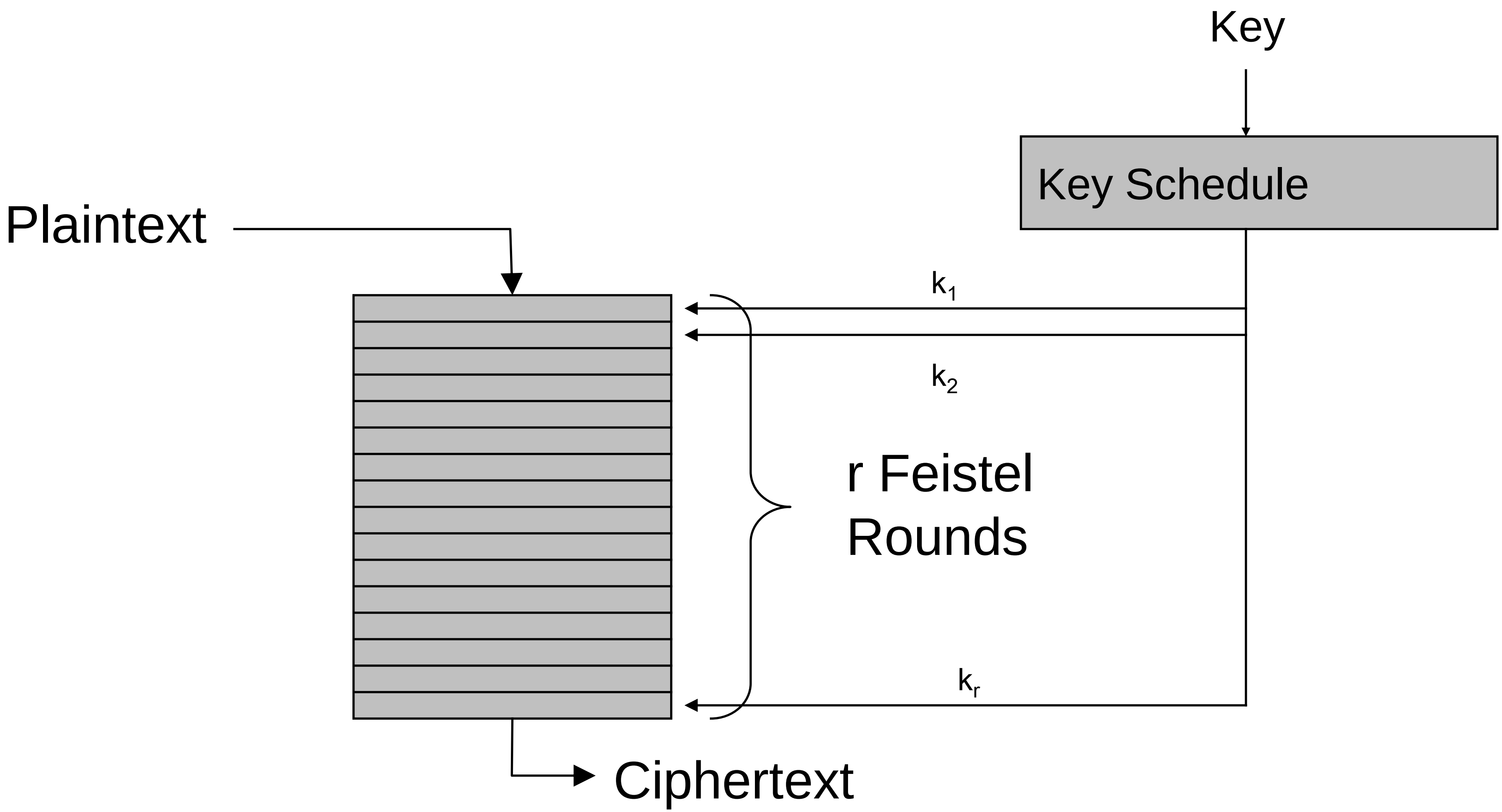


where the *f* function is SP:



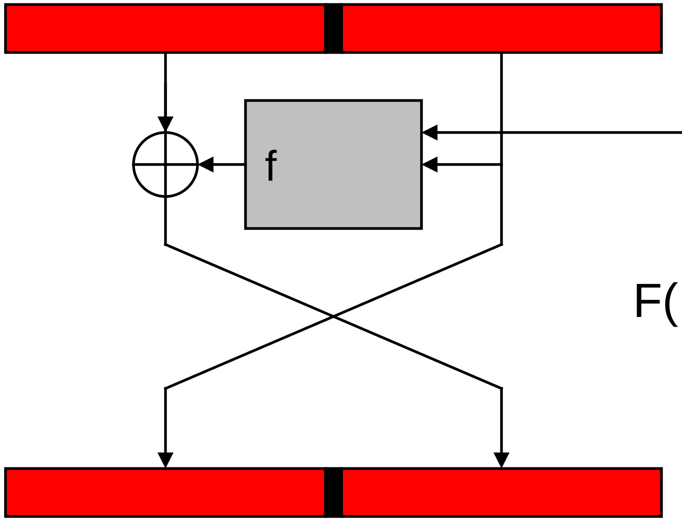
- Lucifer v1: Feistel SP cipher; 64-bit block, 128-bit key, 16 rounds.

Iterated Feistel Cipher



Feistel Round

Graphic courtesy of Josh Benaloh



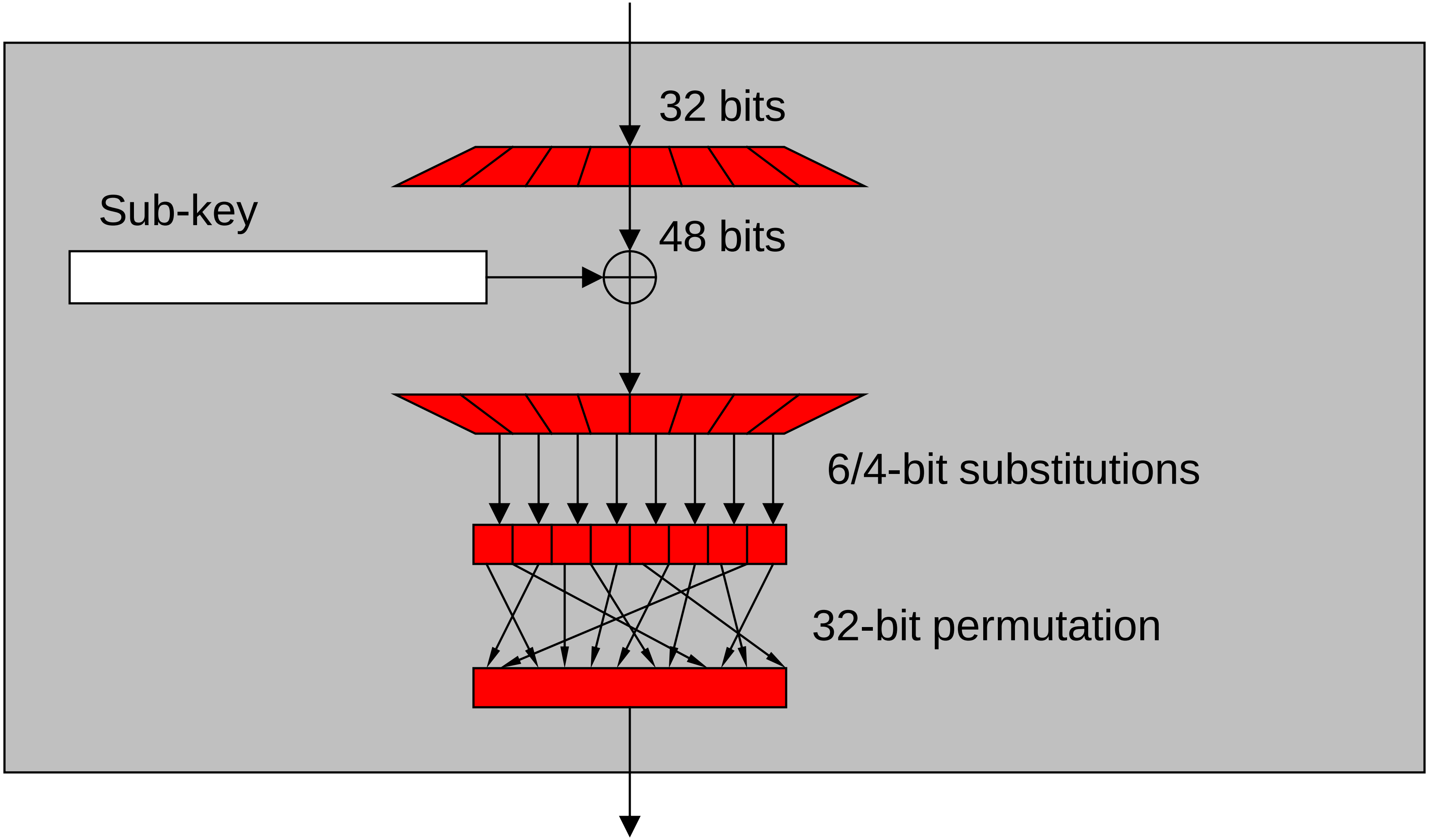
k_i

F(K,X)= non-linear function

Note: If σ_i(L,R)= (L$\oplus$f(E(R) $\oplus$k$_i$) ,R) and τ(L,R)= (R,L), this round is $\tau\sigma_i$(L,R).

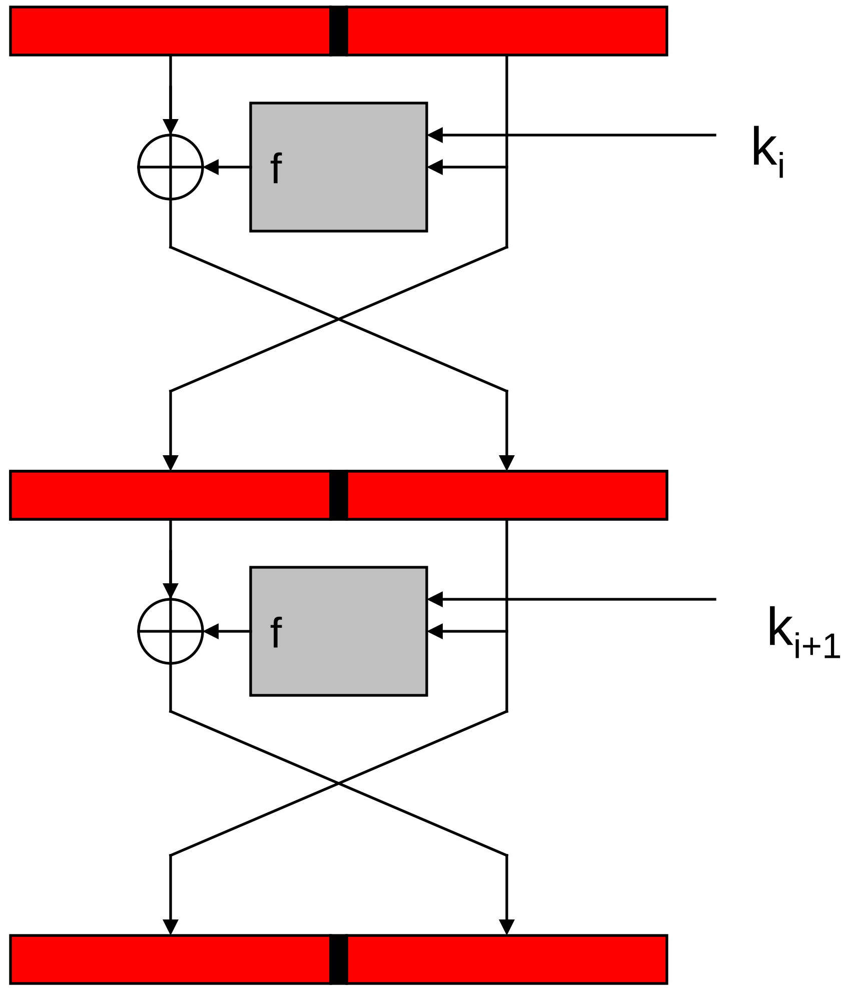
To invert: swap halves and apply same transform with same key: $\sigma_i\tau\tau\sigma_i$(L,R)=(L,R).

DES Round Function

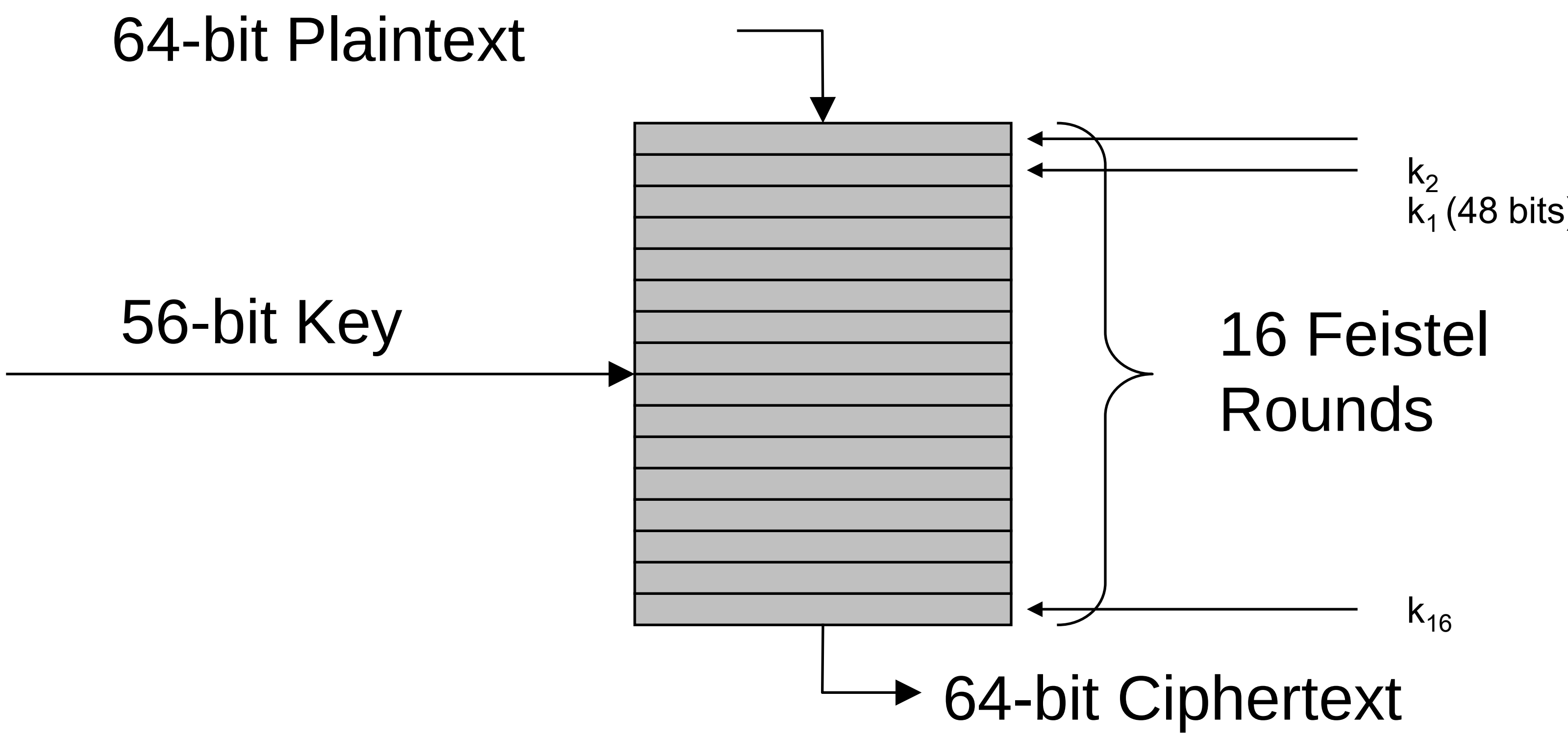


Slide courtesy of Josh Benaloh

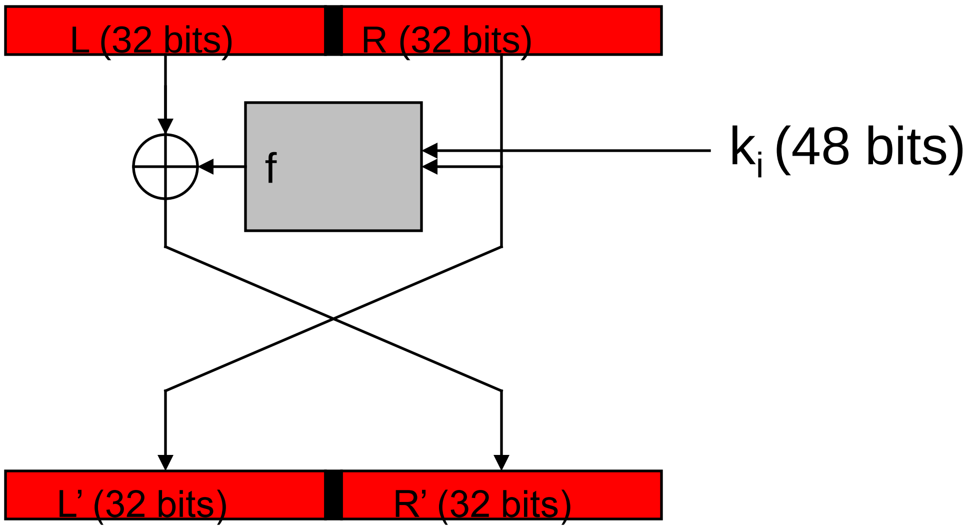
Chaining Feistel Rounds



DES


64-bit Plaintext
56-bit Key
k_2
k_1 (48 bits)
16 Feistel Rounds
k_{16}
64-bit Ciphertext

DES Round



F(K,X)= non-linear function

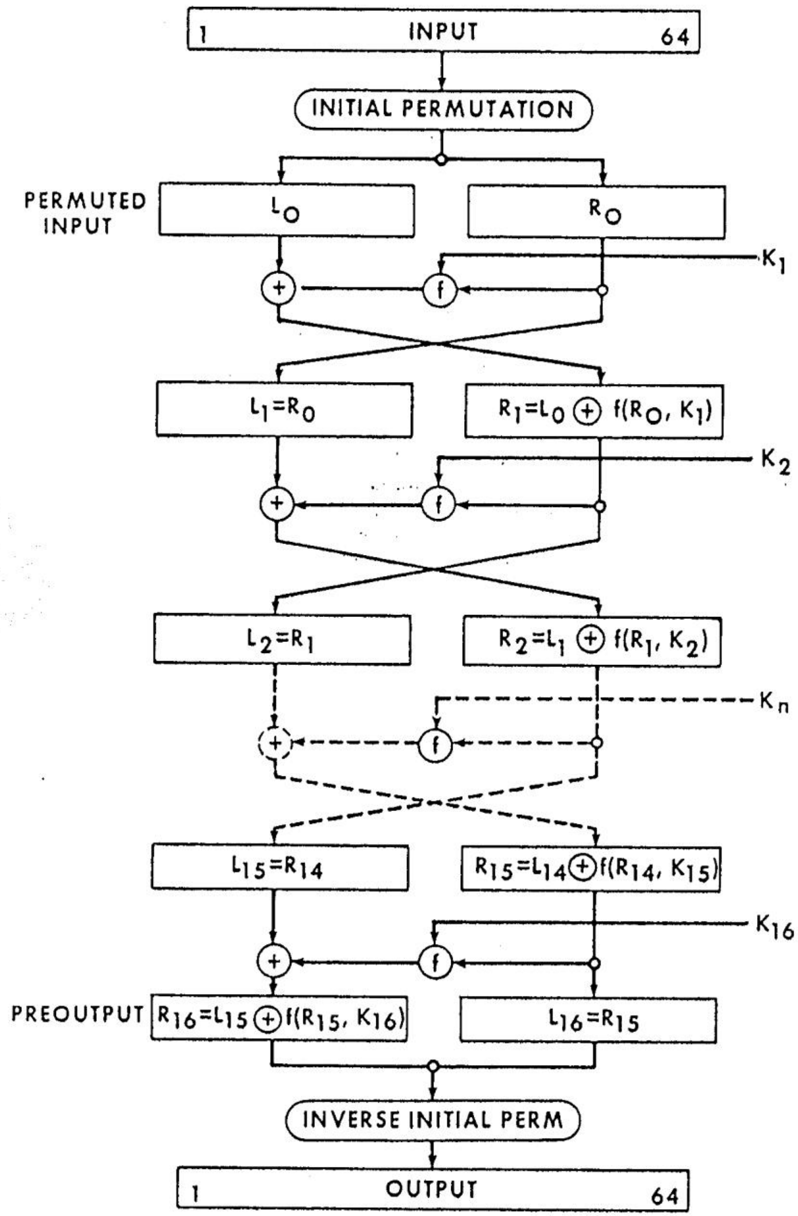


Figure 5.1. Electronic Codebook (ECB) Mode—Enciphering Computation.

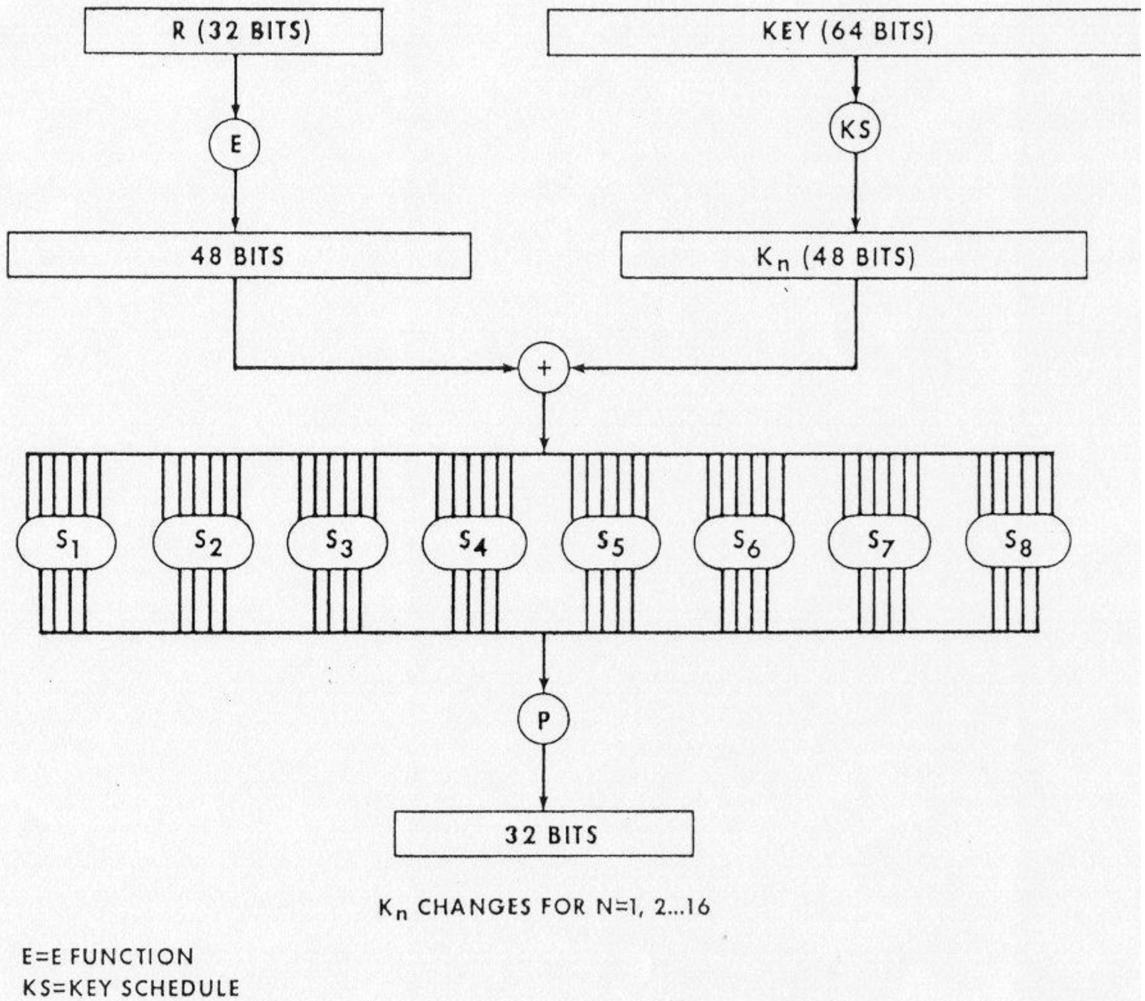


Figure 5.2. Electronic Codebook (ECB) Mode—Calculation of f(R,K).

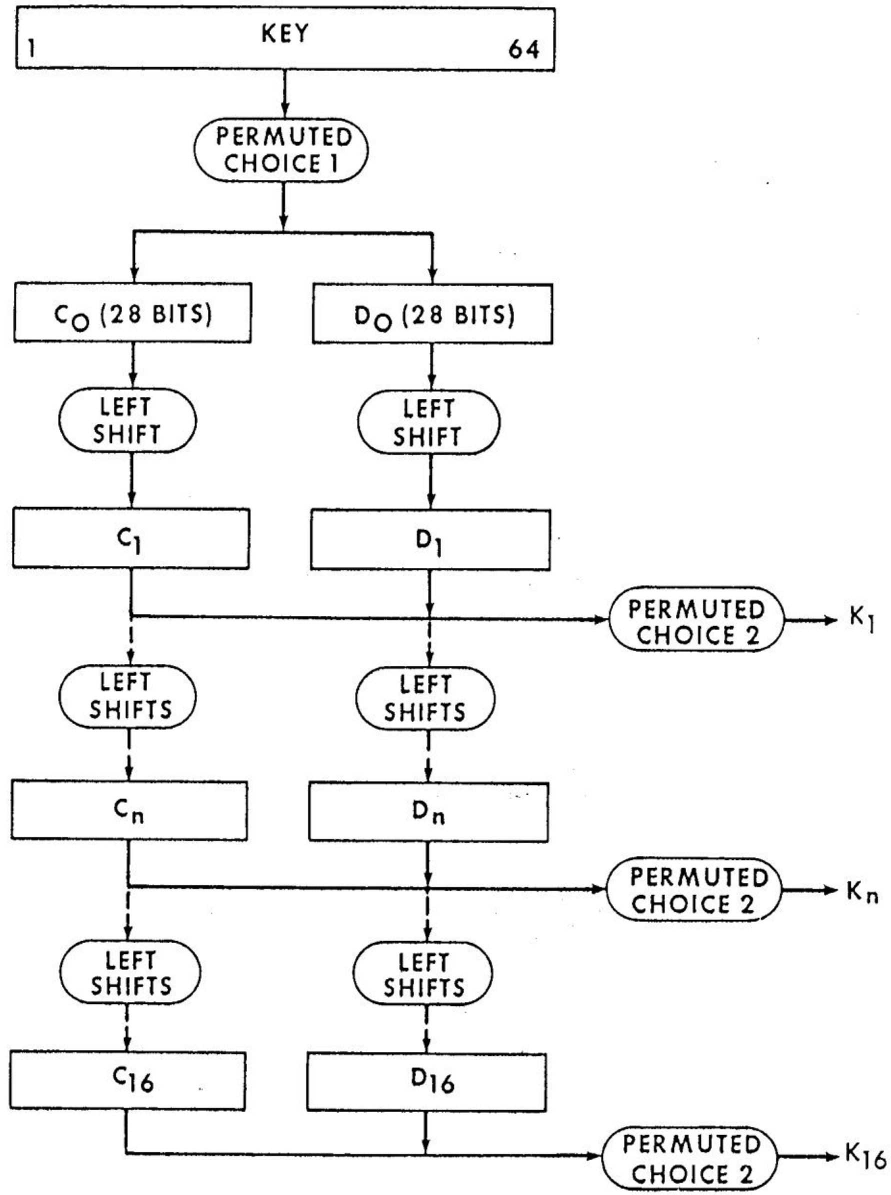


Figure 5.3. Electronic Codebook (ECB) Mode—Key Schedule (KS) Calculation.

DES Described Algebraically

$\sigma_i(L,R) = (L \oplus f(E(R) \oplus k_i), R)$

- k_i is 48 bit sub-key for round i.
- $f(x) = P(S_1 S_2 S_3 \ldots S_8(x))$. Each S –box operates on 6 bit quantities and outputs 4 bit quantities.
- P permutes the resulting 32 output bits.

$\tau(L,R) = (R,L)$.

Each round (except last) is $\tau\sigma_i$. Note that $\tau\tau = \tau^2 = 1 = \sigma_i \sigma_i = \sigma_i^2$.

Full DES is: $DES_K(x) = IP^{-1} \sigma_{16} \tau \ldots \sigma_3 \tau \sigma_2 \tau \sigma_1 IP(x)$.
So its inverse is: $DES_K^{-1}(x) = IP^{-1} \sigma_1 \tau \ldots \sigma_{14} \tau \sigma_{15} \tau \sigma_{16} IP(x)$.

TEA

```
Tea(unsigned K[4], ref unsigned L, ref unsigned R)
{
    unsigned d= 0x9e3779b9;
    unsigned s= 0;
    for(int i=0; i<32;i++) {
        s+= d;
        L+= ((R<<4)+K[0])^(R+s)^((R>>5)+K[1]);
        R+= ((L<<4)+K[2])^(L+s)^((L>>5)+K[3]);
        }
    }
```

DES Key Schedule

$C_0 D_0 = PC_1(K)$

$C_{i+1} = \text{LeftShift}(\text{Shift}_i, C_i)$, $D_{i+1} = \text{LeftShift}(\text{Shift}_i, D_i)$

$K_i = PC_2(C_i \,||\, D_i)$

$\text{Shift}_i = \langle 1,2,2,2,2,2,2,1,2,2,2,2,2,2,1,1 \rangle$

- Note: Irregular Key schedule protects against related key attacks. [Biham, New Types of Cryptanalytic Attacks using Related Keys, TR-753, Technion]

DES Key Schedule

```
pc1[64]
  57 49 41 33 25 17 09 01 58 50 42 34 26 18 10 02
  59 51 43 35 27 19 11 03 60 52 44 36 63 55 47 39
  31 23 15 07 62 54 46 38 30 22 14 06 61 53 45 37
  29 21 13 05 28 20 12 04 00 00 00 00 00 00 00 00

pc2[48]
  14 17 11 24 01 05 03 28 15 06 21 10 23 19 12 04
  26 08 16 07 27 20 13 02 41 52 31 37 47 55 30 40
  51 45 33 48 44 49 39 56 34 53 46 42 50 36 29 32
```

DES Key Schedule

Key schedule round 1

```
10 51 34 60 49 17 33 57  2  9 19 42  3 35 26 25 44 58 59
  1 36 27 18 41

22 28 39 54 37  4 47 30  5 53 23 29 61 21 38 63 15 20 45
 14 13 62 55 31
```

Key schedule round 2

```
  2 43 26 52 41  9 25 49 59  1 11 34 60 27 18 17 36 50 51
 58 57 19 10 33

14 20 31 46 29 63 39 22 28 45 15 21 53 13 30 55  7 12 37
  6  5 54 47 23
```

DES Data

```
S1 (hex)
   e 4 d 1 2 f b 8 3 a 6 c 5 9 0 7
   0 f 7 4 e 2 d 1 a 6 c b 9 5 3 8
   4 1 e 8 d 6 2 b f c 9 7 3 a 5 0
   f c 8 2 4 9 1 7 5 b 3 e a 0 6 d

S2 (hex)
   f 1 8 e 6 b 3 4 9 7 2 d c 0 5 a
   3 d 4 7 f 2 8 e c 0 1 a 6 9 b 5
   0 e 7 b a 4 d 1 5 8 c 6 9 3 2 f
   d 8 a 1 3 f 4 2 b 6 7 c 0 5 e 9

S3 (hex)
   a 0 9 e 6 3 f 5 1 d c 7 b 4 2 8
   d 7 0 9 3 4 6 a 2 8 5 e c b f 1
   d 6 4 9 8 f 3 0 b 1 2 c 5 a e 7
   1 a d 0 6 9 8 7 4 f e 3 b 5 2 c
```

DES Data

```
S4 (hex)
   7 d e 3 0 6 9 a 1 2 8 5 b c 4 f
   d 8 b 5 6 f 0 3 4 7 2 c 1 a e 9
   a 6 9 0 c b 7 d f 1 3 e 5 2 8 4
   3 f 0 6 a 1 d 8 9 4 5 b c 7 2 e

S5 (hex)
   2 c 4 1 7 a b 6 8 5 3 f d 0 e 9
   e b 2 c 4 7 d 1 5 0 f a 3 9 8 6
   4 2 1 b a d 7 8 f 9 c 5 6 3 0 e
   b 8 c 7 1 e 2 d 6 f 0 9 a 4 5 3

S6 (hex)
   c 1 a f 9 2 6 8 0 d 3 4 e 7 5 b
   a f 4 2 7 c 9 5 6 1 d e 0 b 3 8
   9 e f 5 2 8 c 3 7 0 4 a 1 d b 6
   4 3 2 c 9 5 f a b e 1 7 6 0 8 d
```

DES Data

S7 (hex)

4	b	2	e	f	0	8	d	3	c	9	7	5	a	6	1
d	0	b	7	4	9	1	a	e	3	5	c	2	f	8	6
1	4	b	d	c	3	7	e	a	f	6	8	0	5	9	2
6	b	d	8	1	4	a	7	9	5	0	f	e	2	3	c

S8 (hex)

d	2	8	4	6	f	b	1	a	9	3	e	5	0	c	7
1	f	d	8	a	3	7	4	c	5	6	b	0	e	9	2
7	b	4	1	9	c	e	2	0	6	a	d	f	3	5	8
2	1	e	7	4	a	8	d	f	c	9	0	3	5	6	b

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

- Note: DES can be made more secure against linear attacks by changing the order of the S-Boxes: Matsui, On Correlation between the order of S-Boxes and the Strength of DES. Eurocrypt,94.

DES Data

P

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

- Note on applying permutations: For permutations of bit positions, like P above, the table entries consisting of two rows, the top row of which is “in order” means the following. If t is above b, the bit at b is moved into position t in the permuted bit string. For example, after applying P, above, the most significant bit of the output string was at position 16 of the input string.

S Boxes as Polynomials over GF(2)

1,1:
56+4+35+2+26+25+246+245+236+2356+16+15+156+14+146+145+13+135+134+1346+1345+13456+125+1256+1245+123+12356+1234+12346

1,2:
C+6+5+4+45+456+36+35+34+346+26+25+24+246+2456+23+236+235+234+2346+1+15+156+134+13456+12+126+1256+124+1246+1245+12456+123+1236+1235+12356+1234+12346

1,3:
C+6+56+46+45+3+35+356+346+3456+2+26+24+246+245+236+16+15+145+13+1356+134+13456+12+126+125+12456+123+1236+1235+12356+1234+12346

1,4:
C+6+5+456+3+34+346+345+2+23+234+1+15+14+146+135+134+1346+1345+1256+124+1246+1245+123+12356+1234+12346

Legend: C+6+56+46 means $1 \oplus x_6 \oplus x_5 x_6 \oplus x_4 x_6$

Decomposable Systems

- $E_{k1||k2}(x) = E'_{k1}(x) \,||\, E''_{k2}(x)$

m	t	2^{mt}	$m2^t$
2	32	2^{64}	2^{33}
4	16	2^{64}	2^{18}

- Good mixing and avalanche condition

Feistel Ciphers defeat simple attacks

- After 2 to 4 rounds to get flat statistics.
- Parallel system attack
  - Solve for key bits or constrain key bits

$$k_{i(1)}= a_{11}(K)p_1\, c_1 + a_{12}(K)p_2\, c_1 +\ldots+ a_{1N}(K)p_n c_n$$
$$\ldots \qquad \ldots \qquad \ldots \qquad \ldots$$
$$k_{i(m)}= a_{m1}(K)p_1\, c_1 + a_{m2}(K)p_2\, c_1 +\ldots+ a_{mN}(K)p_n c_n$$

- Solving Linear equations for coefficients determining cipher

$$c_1= f_{11}(K)p_1+ f_{12}(K)p_2+\ldots+ f_{1n}(K)p_n$$
$$c_2= f_{21}(K)p_1+ f_{22}(K)p_2+\ldots+ f_{2n}(K)p_n$$
$$\ldots \qquad \ldots \qquad \ldots \qquad \ldots$$
$$c_m= f_{m1}(K)p_1+ f_{m2}(K)p_2+\ldots+ f_{mn}(K)p_n$$

- Even a weak round function can yield a strong Feistel cipher if iterated sufficiently.
  - Provided it's non-linear

DES Attacks: Exhaustive Search

- Symmetry DES($\mathbf{k} \oplus \mathbf{1}$, $\mathbf{x} \oplus \mathbf{1}$)=DES($\mathbf{k}, \mathbf{x}$) $\oplus$ $\mathbf{1}$
- Suppose we know plain/cipher text pair (p,c)

```
for(k=0;k<2^56;k++) {
  if(DES(k,p)==c) {
        printf("Key is %x\n", k);
        break;
        }
}
```

- Expected number of trials (if k was chosen at random) before success: 2^{55}

DES Attacks: Exhaustive Search

- Poor random number generator: 20 bits of entropy
- How long does it take?
- 2^{20} vs 2^{56}
- Second biggest real problem
- First biggest: bad key management

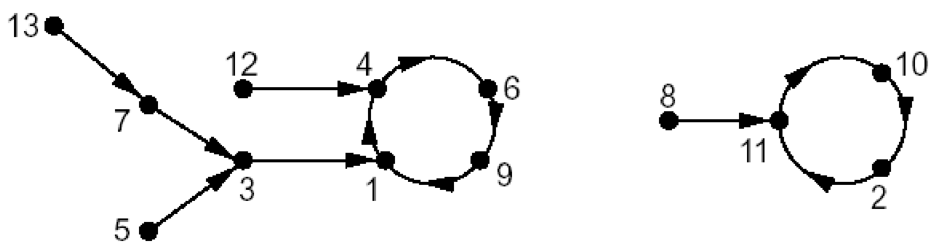
- Symmetric ciphers are said to be secure in practice if no known attack works more efficiently than exhaustive search. Note that the barrier is computational not information theoretic.

Suppose you decide the keyspace is too small?

- Can you increase security by encrypting twice or more?
  - $E'(k_1 \| k_2, x) = E(k_1, E(k_2, x))$
- Answer: Maybe.
- Three times is the charm (triple DES).
- If you do it twice, TMTO attack reduces it to little more than one key search time (if you have a lot of memory).

Random mappings

- Let F_n denote all functions (mappings) from a finite domain of size n to a finite co-domain of size n
- Every mapping is equally likely to be chosen, $|F_n| = n^n$ the probability of choosing a particular mapping is $1/n^n$
- Example. f : {1, 2, ….. 13} → {1, 2, …. 13}



Graphic by Maithili Narasimha

- As n tends to infinity, the following are expectations of some parameters associated with a random point in {1, 2, … n} and a random function from F_n:

  (i) tail length: $\sqrt{(\pi n/8)}$ (ii) cycle length: $\sqrt{(\pi n/8)}$ (iii) rho-length: $\sqrt{(\pi n/2)}$

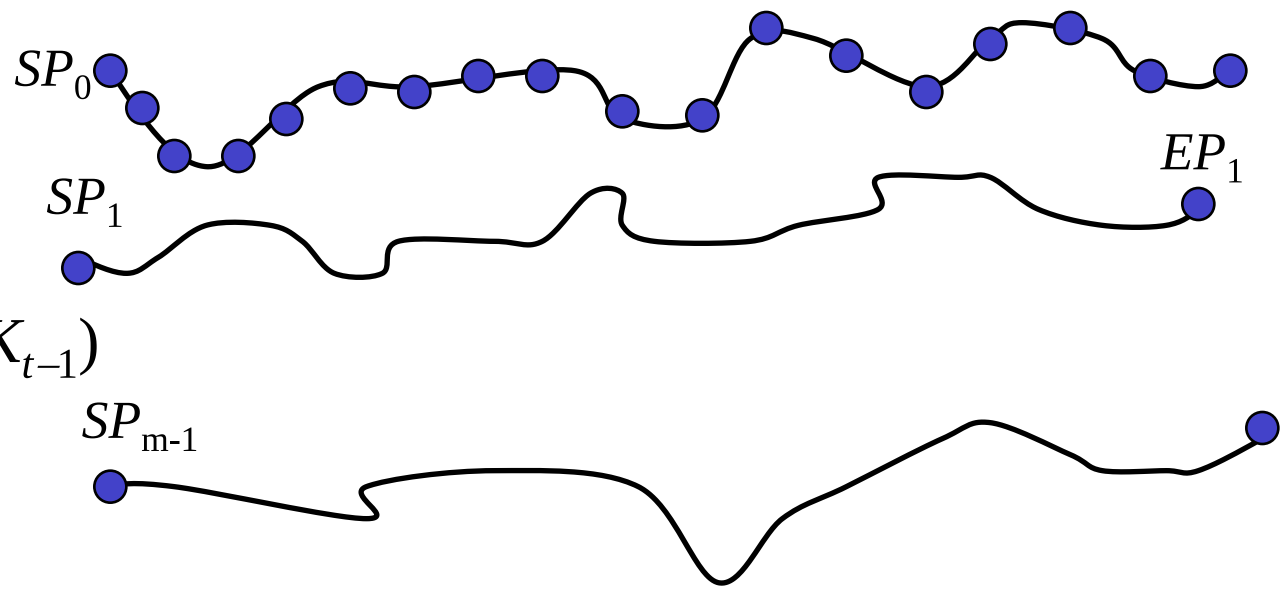
Time memory trade off ("TMTO")

- If we can pre-compute a table of (k, $E_k(x)$) for a fixed x, then given corresponding (x,c) we can find the key in O(1) time.
- Trying random keys takes O(N) time (where N, usually, = 2^k is the number of possible keys)
- Can we balance "memory" and "time" resources?
- It is not a 50-50 proposition. Hellman showed we could cut the search time to $O(N^{(1/2)})$ by precomputing and storing $O(N^{(1/2)})$ values.

Chain of Encryptions

- Assume block length n and key length k are equal: $n = k$
- Construct chain of encryptions:

$$SP = K_0$$
$$K_1 = E(P, SP)$$
$$K_2 = E(P, K_1)$$
$$\vdots$$
$$\vdots$$
$$EP = K_t = E(P, K_{t-1})$$



- Pre-compute m encryption chains, each of length t +1
- Save only the start and end points

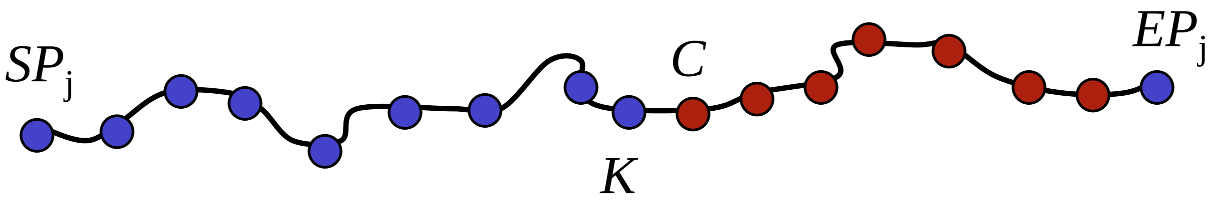
Slide adapted from
Mark Stamp

TMTO Attack

- To attack a particular unknown key K
  - For the same chosen P used to find chains, we know C where $C = E(P, K)$ and K is unknown key
  - Compute the chain (maximum of t steps)

$$X_0 = C, \;\; X_1 = E(P, X_0), \;\; X_2 = E(P, X_1), \ldots$$

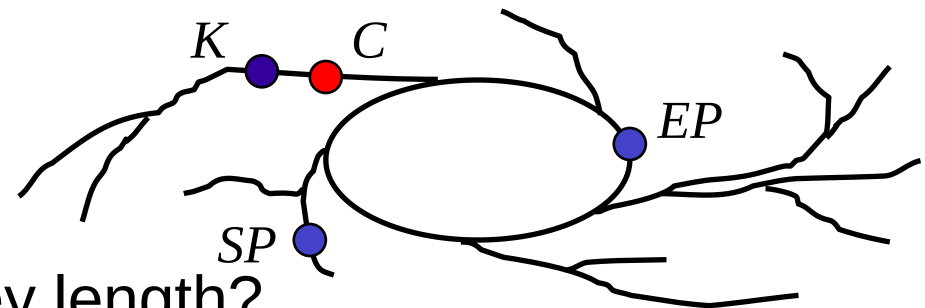
- Suppose for some i we find $X_i = Ep_j$
- Since $C = E(P, K)$ key K should lie before ciphertext C in chain!



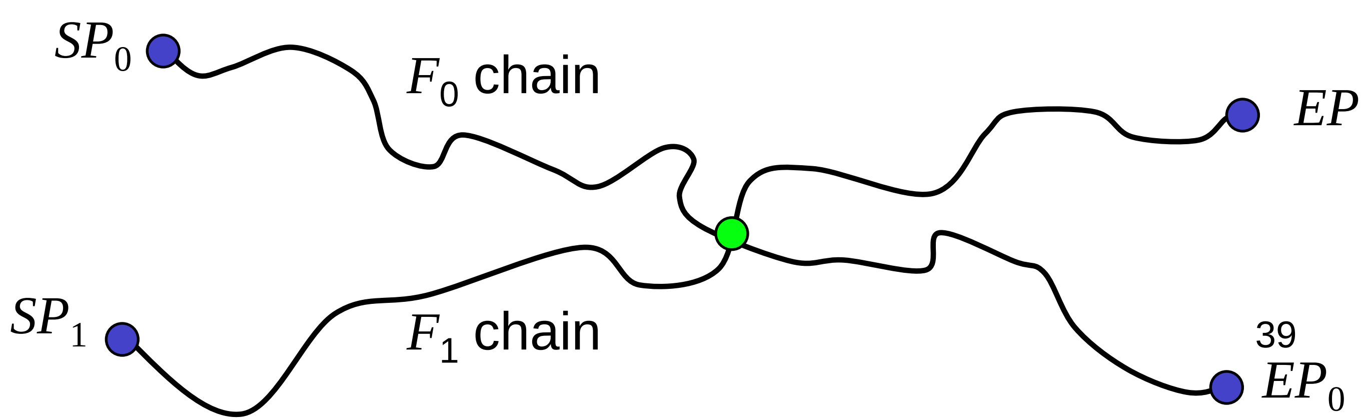
DES TMTO

- Suppose block cipher has $k = 56$
- Suppose we find $m = 2^{28}$ chains each of length $t = 2^{28}$ and no chains overlap (unrealistic)
- Memory: 2^{28} pairs (SP_j, EP_i)
- Time: about 2^{28} (per attack)
  - Start at C, find some EP_j in about 2^{27} steps
  - Find K with about 2^{27} more steps
- Attack never fails!

But things are a little more complicated



- Chains can **cycle** and **merge**
- False alarms, etc.
- What if block size not equal key length?
  - This is easy to deal with
- To reduce merging
  - Compute chain as $F(E(P, K_{i-1}))$ where F permutes the bits
  - Chains computed using different functions can intersect, but they will **not** merge



TMTO in Practice

- Let
  - m = random starting points for each F
  - t = encryptions in each chain
  - r = number of "tables", i.e., random functions F
- Then mtr = total pre-computed chain elements
- Pre-computation is about mtr work
- Each TMTO attack requires
  - About mr "memory" and about tr "time"
- If we choose $m = t = r = 2^{k/3}$ then probability of success is at least 0.55.

Success Probability

- Throw n balls into m urns
- What is expected number of urns that have at least one ball?
  - See Feller, *Intro. to Probability Theory*
- Why is this relevant to TMTO attack?
  - "Urns" correspond to keys
  - "Balls" correspond to constructing chains
- Assuming k-bit key and m,t,r defined as previously discussed
- Then, approximately,

$$P(\text{success}) = 1 - e^{-mtr/k}$$

mtr	$P(\text{success})$
0	0
2^{k-5}	0.03
2^{k-4}	0.06
2^{k-3}	0.12
2^{k-2}	0.22
2^{k-1}	0.39
2^{k}	0.63
2^{k+1}	0.86
2^{k+2}	0.98
2^{k+3}	0.99
∞	1.00

Group theory and DES

- What is the minimum length of a product of involutions from a fixed set required to generate S_n?
- What does this have to do with the number of rounds in a cipher?
- How does this affect the increased security by "enciphering twice" with different keys?
- Theorem (Coppersmith and Grossman): If $\sigma_K(L,R)= (L \oplus f(E(R) \oplus K, R)$, $<\tau, \sigma_K>= A_N$, $N= 2^n$.
- Note (Netto): If a and b are chosen at random from S_n there is a good chance (~¾) that $<a,b>= A_n$ or S_n .

DES is not a group

- Set $E_1(x)= DES_{0xffffffffffffff}(x)$, $E_0(x)= DES_{0x00000000000000}(x)$.
- $F(x)= E_1(E_0(x))$.
- There is an x: $F^m(x)=x$, $m \sim 2^{32}$, a cycle length.
- If $|F|=n$, $m \mid n$.
- Suppose DES is closed under composition so $F=E_k=DES_k$.
- $E_k^i= E_k^j$, $E_k^{(j-i)}= I$. $0<=i<j<=2^{56}$.
- Coppersmith found lengths of cycles for 33 plaintexts and the LCM of these cycle lengths > 2^{277}.

If DES were a group…

- Suppose $E_{K1}(E_{K2}(x))=E_{K3}(x)$, that there are N possible keys, plaintexts and ciphertexts and that for a given plaintext-ciphertext pair there is only one possible key then there is a birthday attack that finds the key in $O(N^{(1/2)})$.

- Construct $D_{K1}(x)$ for $O(N^{(1/2)})$ random keys, K1 and $E_{K2}(x)$ for $O(N^{(1/2)})$ random keys, K2. If there is a match, $c=E_{K1}(E_{K2}(x))$. This has the same effect as finding K3.

DES Key Schedule

$C_0D_0 = PC_1(K)$

$C_{i+1} = \text{LeftShift}(\text{Shift}_i, C_i)$, $D_{i+1} = \text{LeftShift}(\text{Shift}_i, D_i)$,

$K_i = PC_2(C_i \| D_i)$

$\text{Shift}_i = \langle 1,2,2,2,2,2,2,1,2,2,2,2,2,2,1,1 \rangle$

Note: Irregular Key schedule protects against related key attacks. [Biham, New Types of Cryptanalytic Attacks using Related Keys, TR-753, Technion]

Weak Keys

- DES has:
  - Four weak keys k for which $E_k(E_k(m)) = m$.
  - Twelve semi-weak keys which come in pairs k_1 and k_2 and are such that $E_{k1}(E_{k2}(m)) = m$.
  - Weak keys are due to "key schedule" algorithm

How Weak Keys Arise

- A 28 bit quantity has potential symmetries of period 1,2,4,7, and 14.

- Suppose each of C_0 and D_0 has a symmetry of period 1; for example C_0 =0x0000000, D_0= 0x1111111. We can easily figure out a master key (K) that produces such a C_0 and D_0.

- Then $DES_K(DES_K(x))=x$.

Interlude: Useful Math for Boolean Functions

- Algebraic Representations
- Linear Functions
- Affine approximations
- Bent Functions: functions furthest from linear
- Hadamard transforms
- MDS, linear codes, RS codes
- Random Functions
- Correlation and Correlation Immunity

- Some Notation:
  - Let $L_1(P) \oplus L_2(C) = L_3(K) \oplus c$ with probability p_i
  - $\epsilon_i = |1- p_i|$ called the “bias”

Boolean Functions

- For a set of Boolean functions Δ, $d(f,g)=\#\{X|f(X) \neq g(X)\}$.
- *Distance*: For Boolean function f(X) and g(X), $d(f,\Delta)= \min_{[g(X)\epsilon\Delta]} d(f,g)$
- *Affine function*: $h(x)= a_1x_1\oplus a_2x_2 \oplus \ldots\oplus a_nx_n+c$
- *nl(f)* denotes the minimum distance between f(X) and the set of affine functions Δ_{affine}. *nl(f)= d(f,* Δ_{affine}*)*, Δ_{affine}= *RM(1,n).*
- *Balance*: f(X) is balanced iff there is an equal number of 0's and 1's in the output of f(X).

Algebraic Representations

- *Algebraic normal form* (ANF):

$$f(X) = a_0 \oplus \left(\bigoplus_{i=1}^{i=n} a_i x_i\right)$$
$$\oplus \left(\bigoplus_{1\le i\neq j\le n} a_{ij} x_i x_j\right) \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n$$

- *Degree*: deg(f),the highest degree term in ANF.
  - Example

    $f(X)= x_1+x_2$, deg(f)=1

    $g(X)=x_1x_2$, deg(g)=2
- Lagrange Interpolation Theorem: Every function in n variables can be expressed as a polynomial (hence ANF).
- Degree is not the best measure of nonlinearity.

  $f(x_1,\ldots,x_n)= x_1 \oplus \ldots \oplus x_n \oplus x_1\ldots x_n$ has high degree but differs from a perfectly linear function at only 1 of 2^n possible arguments.

Correlation Immunity

- f(X) is *correlation immune* of order t if f(X) is not correlated with any t-subset of $\{x_1, x_2, \ldots, x_n\}$. That is,

$$\Pr(f(X)=0 \mid x_{i_1}=b_{i_1},\ldots,x_{i_t}=b_{i_t}) = \Pr(f(X)=0)$$

- f(X) is *t-resilient* if f(X) is balanced and f(X) is correlation immune of order t.

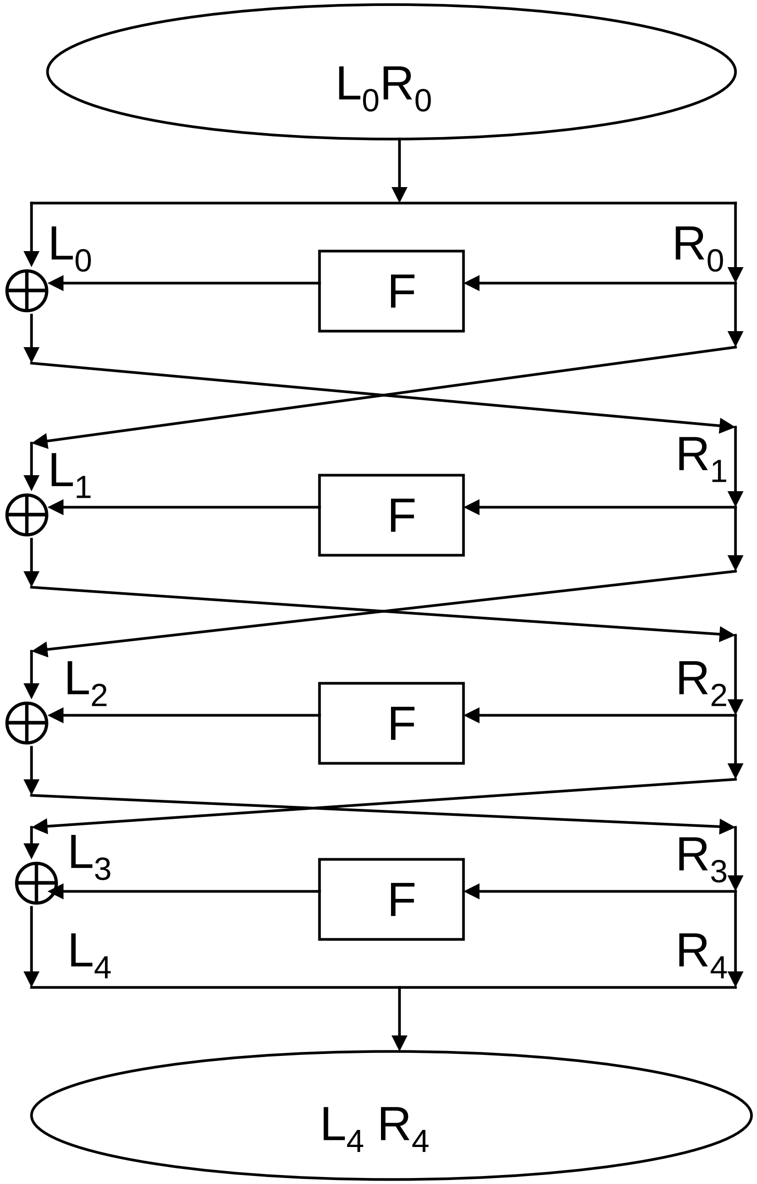
$$\Pr(f(X)=0 \mid x_{i_1}=b_{i_1},\ldots,x_{i_t}=b_{i_t}) = \Pr(f(X)=0) = \frac{1}{2}$$

- Theorem: Let $f(x_1, x_2, \ldots x_n)$ be a balanced boolean function of algebraic degree d in n variables which is t-th order correlation immune then
  - $d+t \leqq n-1$, $1 \leqq t \leqq n-2$
  - $d+t \leqq n$, $t=n-1$

Mathematics of Boolean Functions

- Correlation
  - $c(f,g) = P[f(x)=g(x)] - P[f(x) \neq g(x)]$.
  - $P[f(x)=g(x)] = .5(1+c(f,g))$
- Hadamard
  - $S_f(w) = 2^{-n}\Sigma_x (-1)^{f(x)+w \cdot x}$
- Parseval
  - $.\Sigma_w S_f(w)^2=1$
- Bent functions
  - Furthest from linear (all Hadamard coefficients are equal)

Simplified DES



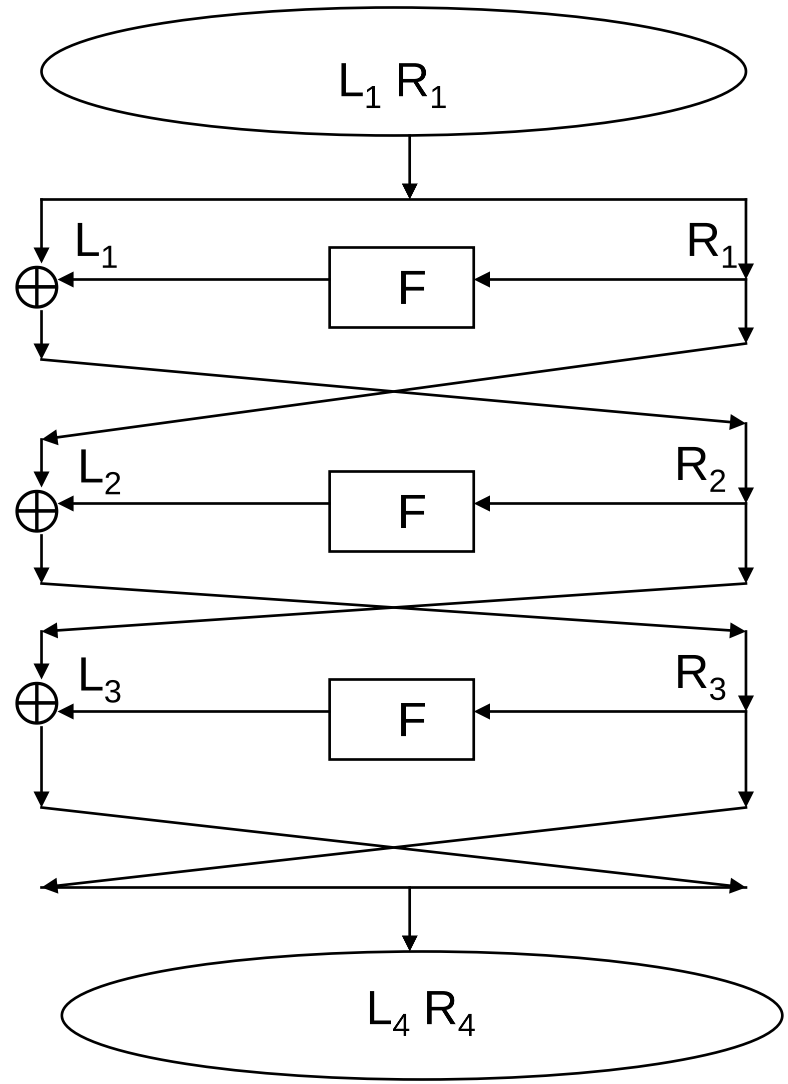
- $L_{i+1} = R_i$, each 6 bits.
- $R_{i+1} = L_i \oplus f(R_i, K_i)$
- K is 9 bits.
- $E(x) = (x_1\ x_2\ x_4\ x_3\ x_4\ x_3\ x_5\ x_6)$
- S_1
  - 101 010 001 110 011 100 111 000
  - 001 100 110 010 000 111 101 011
- S_2
  - 100 000 110 101 111 001 011 010
  - 101 011 000 111 110 010 001 100
- K_i is 8 bits of K starting at i^{th} bit.

Differential Cryptanalysis – 3R

- $L_4 \oplus R_1 = f(k_3, R_2)$. .... (1)
- $R_4 \oplus L_3 = f(k_4, R_3)$. .... (2)
- $L_4 = R_3$, $L_2 = R_1$, $L_3 = R_2$.

- 1& 2→ $R_4 \oplus L_3 \oplus R_2 \oplus L_1 = f(k_2, R_1) \oplus f(k_4, R_3)$.
- $L_3 = R_2$→ $R_4 \oplus L_1 = f(k_2, R_1) \oplus f(k_4, R_3)$.

- $R_4 \oplus L_1 = f(k_2, R_1) \oplus f(k_4, R_3)$. ....(3)
- $R_4^* \oplus L_1^* = f(k_2, R_1^*) \oplus f(k_4, R_3^*)$. ....(4)
- 3&4→ $R_4' \oplus L_1' = f(k_2, R_1^*) \oplus f(k_4, R_3^*) \oplus f(k_2, R_1^*) \oplus f(k_4, R_3^*)$.
- $R_1 = R_1^*$ →$R_4' \oplus L_1' = f(k_4, R_3) \oplus f(k_4, R_3^*)$.



Differential Cryptanalysis – 3R

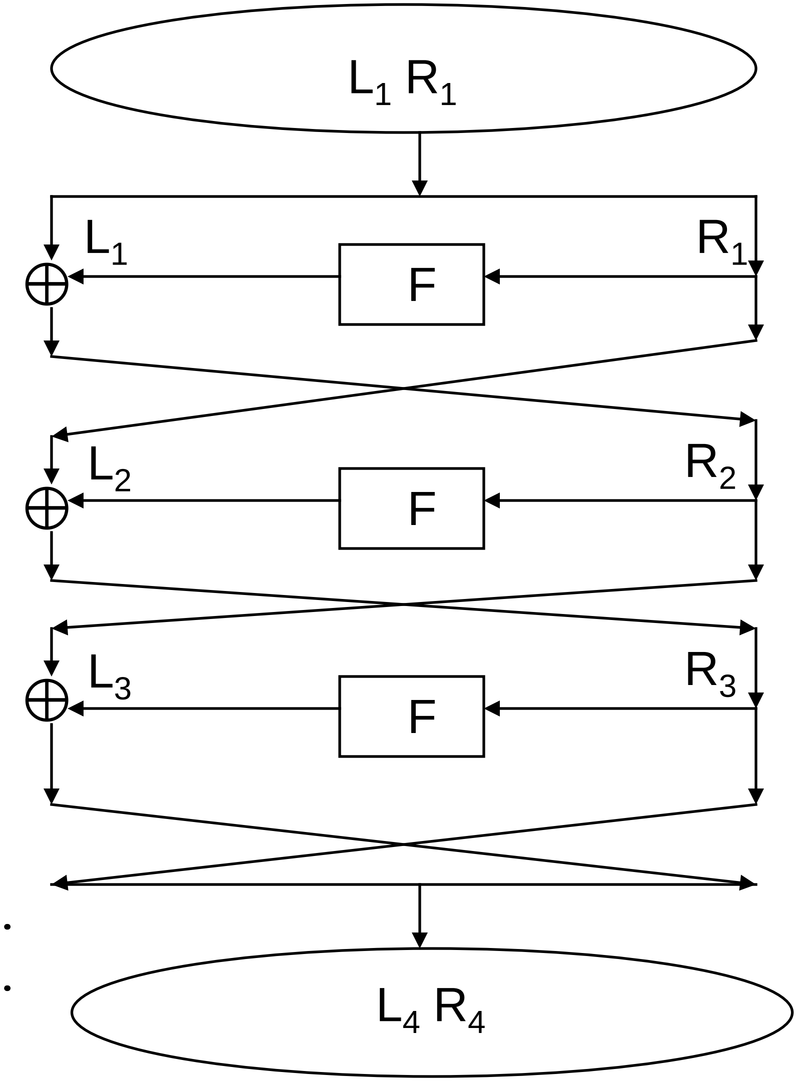
L_1, R_1 : 000111 011011
L_1^*, R_1^*: 101110 011011
L_1', R_1': 101001 000000

L_4, R_4 : 000011 100101
L_4^*, R_4^*: 100100 011000
L_4', R_4': 100111 111101

$E(L_4)$: 0000 0011
$E(L_4')$: 1010 1011
$R_4' \oplus L_1'$: 111 101 $\oplus$ 101 001= 010 100.
S_1': 1010 → 010(1001,0011).
S_2': 1011 → 100(1100,0111).

$(E(L_4)\oplus k_4)_{1..4}$=1001|0011, k_4= 1001|0011.
$(E(L_4)\oplus k_4)_{5..8}$= 1100|0111,$k_4$= 1111|0100.

K= 00x001101



Differential Cryptanalysis 4R

Pick

L_0', R_0': 011010 001100.

Then

$E(R_0')$: 0011 1100.

0011 → 011 with p=3/4

1100 → 010 with p=1/2

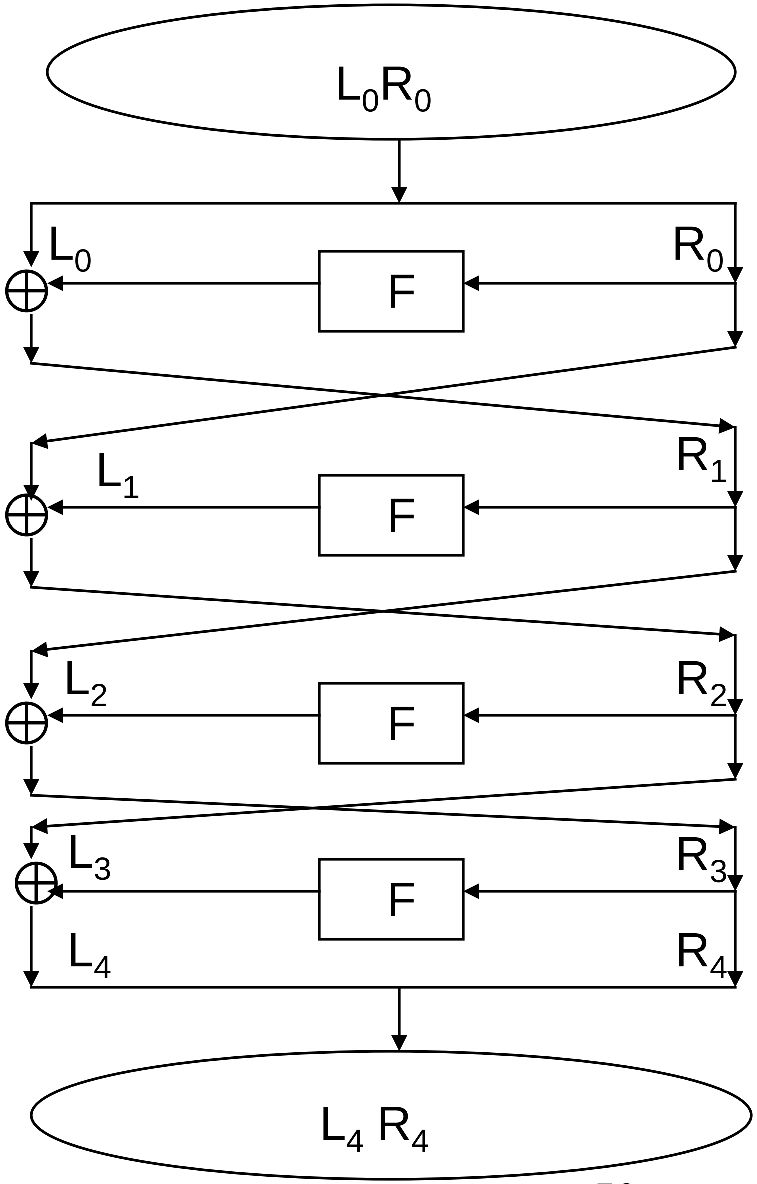
So

$f(R_0', k_1)$= 011 010, p=3/8.

Thus

L_1', R_1': 001100 000000, p=3/8.

- 3/8 of the pairs with this differential produce this result. 5/8 scatter the output differential at random. These "vote" for 1100 and 0010.



Differential Cryptanalysis of DES

- Best 16 rounds attack uses 13 round approximation
  - Requires 2^{47} texts
  - Not much better than exhaustive search
- Converting Chosen Plaintext to Corresponding plaintext attack
  - If m pairs are required for chosen plaintext attack then $\sqrt{(2m)}\, 2^{32}$ are required for corresponding plaintext

Comments on Differential Cryptanalysis of full DES

# Rounds	Needed pairs	Analyzed Pairs	Bits Found	# Char rounds	Char prob	S/N	Chosen Plain
4	2^3	2^3	42	1	1	16	2^4
6	2^7	2^7	30	3	1/16	2^{16}	2^8
8	2^{15}	2^{13}	30	5	1/10486	15.6	2^{16}
16	2^{57}	2^5	18	15	$2^{-55.1}$	16	2^{58}

DES S-Box Design Criteria

- No S-box is linear or affine function of its input.
- Changing one bit in the input of an S-Box changes at least two output bits.
- S-boxes were chosen to minimize the difference between the number of 1's and 0's when any input bit is held constant.
- $S(X)$ and $S(X \oplus 001100)$ differ in at least 2 bits
- $S(X) \neq S(X \oplus 11xy00)$

Comments on effect of components on Differential Cryptanalysis

- E
  - Without expansion, there is a 4 round iterative characteristic with p= 1/256
- P
  - Major influence. If P=I, there is a 10 round characteristic with p= $2^{-14.5}$ (but other attacks would be worse).
- S order
  - If S1, S7 and S4 were in order, there would be a 2 round iterative characteristic with p= 1/73. However, Matsui found an order (24673158) that is better and also better against Linear crypto. Optimum order for LC resistance: 27643158.
- S properties
  - S boxes are nearly optimum against differential crypto

Linear Cryptanalysis

- Invented by Mitsuru Matsui in 1993.
- 16-round DES can be attacked using 2^{43} known plaintexts - get 26 bits, brute force the remaining 30 bits
  - $2^{43} = 9 \times 10^{12}$ = 9 trillion known plaintext blocks
- Also exploits biases in S-boxes, which were not designed against the attack
- A DES key was recovered in 50 days using 12 HP9735 workstations in a lab setting

Linear Cryptanalysis

- Basic idea:
  - Suppose $\alpha_i(P) \oplus \beta_i(C) = \gamma_i(k)$ holds with γ_i, linear, for i= 1,2,…,m.
  - Each equation imposes a linear constraint and reduces key search by a factor of 2.
  - Guess (n-m-1) bits of key. There are $2^{(n-m-1)}$. Use the constraints to get the remaining keys.

- Can we find linear constraints in the “per round” functions and knit them together?
- No! Per Round functions do not have linear constraints.

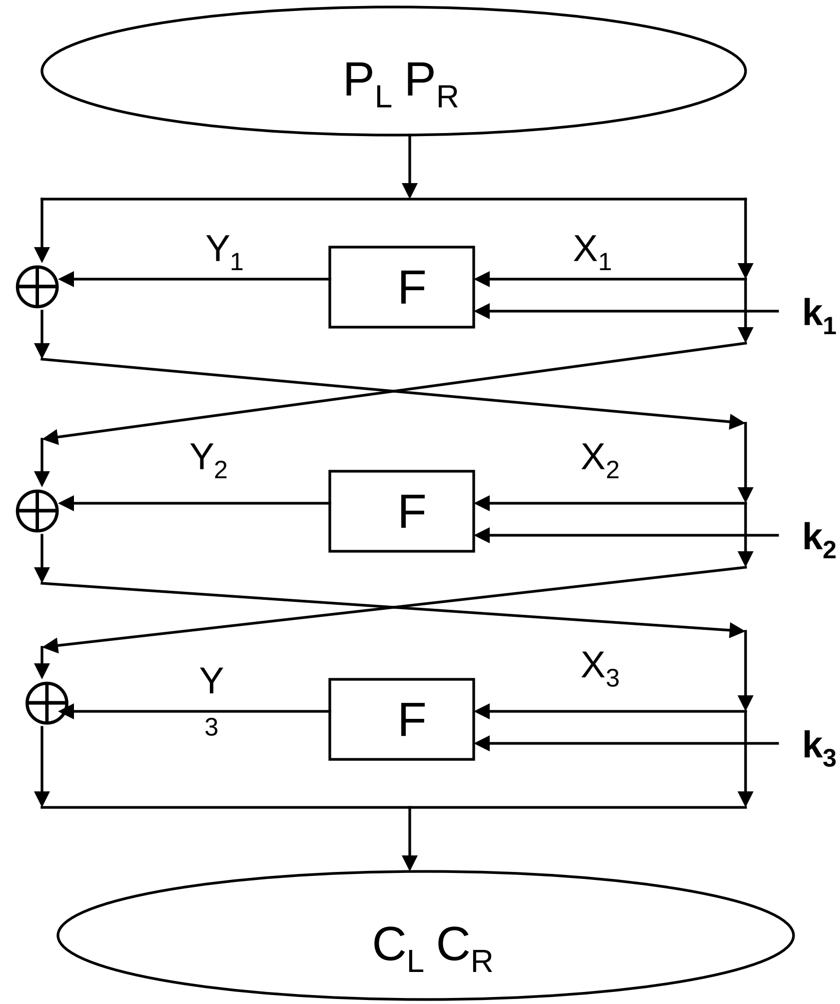
Linear Cryptanalysis

- Next idea
  - Can we find $\alpha(P) \oplus \beta(C) = \gamma(k)$ which holds with γ, linear, with probability p?
  - Suppose $\alpha(P) \oplus \beta(C) = \gamma(k)$, with probability p>.5.
  - Collect a lot of plain/cipher pairs.
  - Each will "vote" for $\gamma(k)=0$ or $\gamma(k)=1$.
  - Pick the winner.

p= $1/2+\epsilon$ requires $c\epsilon^{-2}$ texts (we'll see why later). ϵ is called "bias".

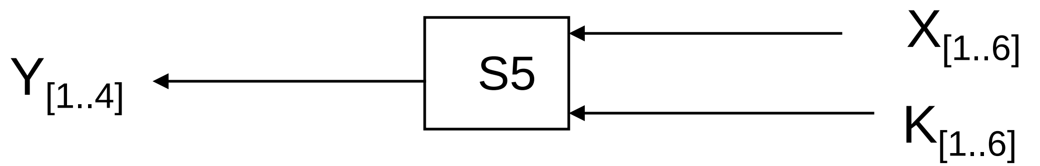
Linear Cryptanalysis Notation

- Matsui numbers bits from right to left, rightmost bit is bit 0. FIPS (and everyone else) goes from left to right starting at 1. I will use the FIPS conventions. To map Matsui positions to everyone else's:
  - M(i)= 64-EE(i). For 32 bits make the obvious change.
- Matsui also refers to the two potions of the plan and ciphertext as
- (P_H, P_L), (C_H, C_L) we'll stick with (P_L, P_R), (C_L, C_R).



Linear and near linear dependence

- Here is a linear relationship over GF(2) in S5 that holds with probability 52/64 (from $NS_5(010000,1111) = 12$:



- $X[2] \oplus Y[1] \oplus Y[2] \oplus Y[3] \oplus Y[4] = K[2] \oplus 1$,
- Sometimes written: $X[2] \oplus Y[1,2,3,4] = K[2] \oplus 1$

- You can find relations like this using the “Boolean Function” techniques we describe a little later

- Inside full round (after applying P), this becomes

  $X[17] \oplus F(X,K)[3,8,14,25] = K[26] \oplus 1$

Linear Cryptanalysis of 3 round DES

$X[17] \oplus Y[3,8,14,25] = K[26] \oplus 1$, p= 52/64

- Round 1

$X_1[17] \oplus Y_1[3,8,14,25] = K_1[26] \oplus 1$

$P_R[17] \oplus P_L[3,8,14,25] \oplus R_1[3,8,14,25] =$
$K_1[26] \oplus 1$

- Round 3

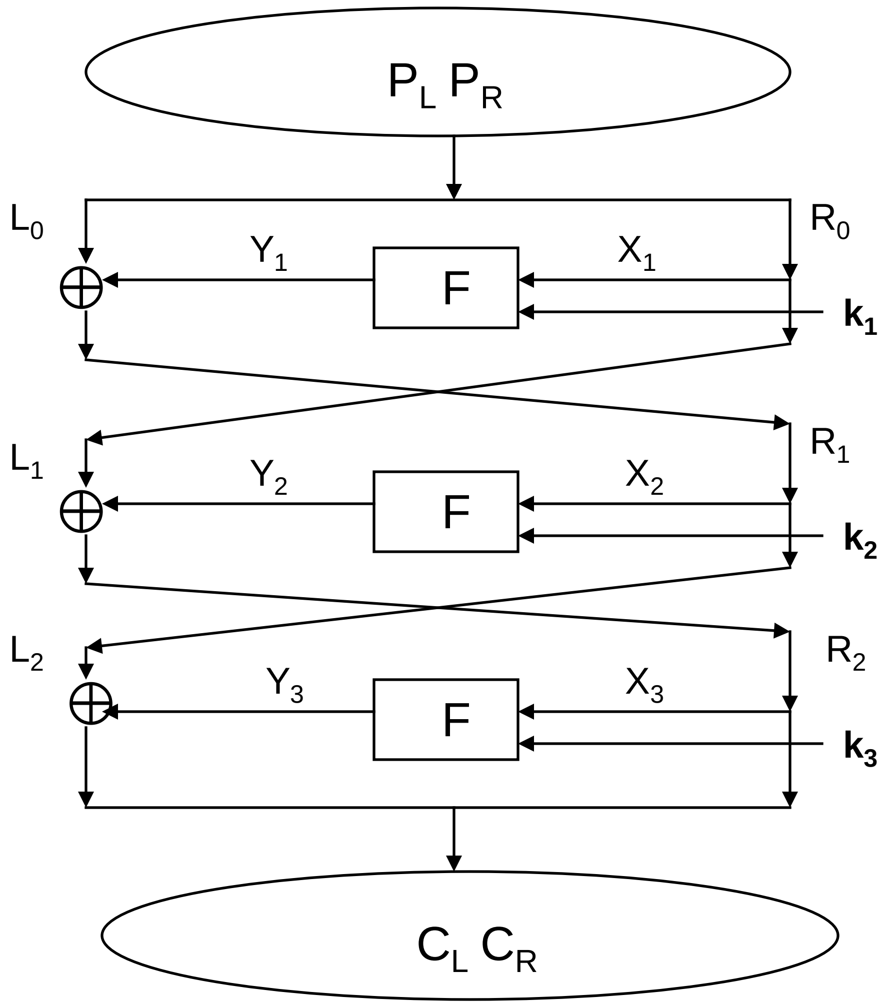
$X_3[17] \oplus Y_3[3,8,14,25] = K_3[26] \oplus 1$

$R_1[3,8,14,25] \oplus C_L[3,8,14,25] \oplus C_R[17] =$
$K_3[26] \oplus 1$

- Adding the two get:

$P_R[17] \oplus P_L[3,8,14,25] \oplus C_L[3,8,14,25] \oplus$
$C_R[17] = K_1[26] \oplus K_3[26]$

Thus holds with p= $(52/64)^2 + (12/64)^2 = .66$



Piling Up Lemma

- Let X_i $(1 \leqq i \leqq n)$ be independent random variables whose values are 0 with probability p_i. Then the probability that $X_1 \oplus X_2 \oplus ... \oplus X_n = 0$ is

$$½+2^{n-1} \prod_{[1,n]} (p_i-1/2)$$

Proof:

By induction on n. It's tautological for n=1.

Suppose $Pr[X_1 \oplus X_2 \oplus ... \oplus X_{n-1}= 0]= q= ½+2^{n-2} \prod_{[1,n-1]} (p_i-1/2)$. Then

$Pr[X_1 \oplus X_2 \oplus ... \oplus X_n= 0]= qp_n +(1-q)(1-p_n)=½+2^{n-1} \prod_{[1,n]} (p_i-1/2)$ as claimed.

Mathematics of biased voting

Central Limit Theorem. Let X, X_1 , … , X_n be independent, identically distributed random variables and let $S_n = X_1 + X_2 + \dots + X_n$. Let μ= E(X) and σ^2=E((X-μ)^2). Finally set $T_n= (S_n-n\mu)/(\sigma\sqrt{n})$, $n(x)= 1/(\sqrt{2\pi}) \exp(-x^2/2)$ and

$$N(a,b)= \int_{[a,b]} n(x)\, dx.$$

Then

$$\Pr(a \leqq T_n \leqq b)= N(a,b).$$

n is called the Normal Distribution and is symmetric around x=0. $N(-\infty,0)$= ½.

N(-.5, .5)=.38, N(-.75,.75)= .55, N(-1,1)= .68, N(-2,2)=.9546, N(-3,3)= .9972

Application of CLT to LC

- $p = \frac{1}{2}+\epsilon$, $1-p = \frac{1}{2}-\epsilon$. Let $L(k,P,E_k(P))=0$ be an equation over GF(2) that holds with probability p. Let X_i be the outcome (1 if true, 0 if false) of an experiment picking P and testing whether L holds for the real k.
- $E(X_i)= p$, $E((X_i-p)^2)= p(1-p)^2 + (1-p)(0-p)^2= p(1-p)$. Let T_n be as provided in the CLT.
- Fixing n, what is the probability that more than half the X_i are 1 (i.e.- What is the probability that n random equations vote for the right key)?
- This is just $\Pr(T_n \geqq -\epsilon\sqrt{n}/\sqrt{(1/4 - \epsilon^2)})$. If $n=\delta^2\epsilon^{-2}$, this is just
- $\Pr(T_n \geqq -\delta/\sqrt{(1/4 - \epsilon^2)})$ or, if ϵ is small $\Pr(T_n \geqq -2\delta)$.
- Some numerical values: $\delta = .25$, $N(-.5, \infty) = .69$, $\delta = .5$, $N(-1, \infty) = .84$,

$\delta = 1$, $N(-2, \infty) = .98$, $\delta = 1.5$, $N(-3, \infty) = .999$.

Matsui's Per Round Constraints

Label	Equation	Pr
A	$X[17] \oplus Y[3,8,14,25]=K[26]$	12/64
B	$X[1,2,4,5] \oplus Y[17]=K[2,3,5,6]$	22/64
C	$X[3] \oplus Y[17]=K[4]$	30/64
D	$X[17] \oplus Y[8,14,25]=K[26]$	42/64
E	$X[16,20] \oplus Y[8,14,25]=K[25,29]$	16/64

Matsui: Linear Cryptanalysis Method for DES Cipher. Eurocrypt, 98.

15 Round Linear Approximation

Pattern: E-DCA-ACD-DCA-A. Note $L_i=R_{i-1}$, $L_i \oplus R_{i+1}=L_i \oplus L_{i+2}$.

1	$P_L[8,14,25]$	$\oplus$	$R_2[8,14,25]$	$\oplus$	$P_R[16,20]$	=	$K_1[23,25]$
3	$L_3[8,14,25]$	$\oplus$	$R_4[8,14,25]$	$\oplus$	$R_3[17]$	=	$K_3[26]$
4	$L_4[17]$	$\oplus$	$R_5[17]$	$\oplus$	$R_4[3]$	=	$K_4[4]$
5	$L_5[3,8,14,25]$	$\oplus$	$R_6[3,8,14,25]$	$\oplus$	$R_5[17]$	=	$K_5[26]$
7	$L_7[3,8,14,25]$	$\oplus$	$R_8[3,8,14,25]$	$\oplus$	$R_7[17]$	=	$K_7[26]$
8	$L_8[17]$	$\oplus$	$R_9[17]$	$\oplus$	$R_8[3]$	=	$K_8[4]$
9	$L_9[8,14,25]$	$\oplus$	$R_{10}[8,14,25]$	$\oplus$	$R_9[17]$	=	$K_9[26]$
11	$L_{11}[8,14,25]$	$\oplus$	$R_{12}[8,14,25]$	$\oplus$	$R_{11}[17]$	=	$K_{11}[26]$
12	$L_{12}[17]$	$\oplus$	$R_{13}[17]$	$\oplus$	$R_{12}[3]$	=	$K_{12}[4]$
13	$L_{13}[3,8,14,25]$	$\oplus$	$R_{14}[3,8,14,25]$	$\oplus$	$R_{13}[17]$	=	$K_{13}[26]$
15	$L_{15}[3,8,14,25]$	$\oplus$	$C_L[3,8,14,25]$	$\oplus$	$C_R[17]$	=	$K_{15}[26]$

15 Round Linear Approximation

Adding and canceling:

$$P_L[8,14,25] \oplus P_R[16,20] \oplus C_L[3,8,14,25] \oplus C_R[17] =$$
$$K_1[23,25] \oplus K_3[26] \oplus K_4[4] \oplus K_5[26] \oplus K_7[26] \oplus K_8[4]$$
$$\oplus K_9[26] \oplus K_{11}[26] \oplus K_{12}[4] \oplus K_{13}[26] \oplus K_{15}[26]$$

which holds (by Piling-up Lemma) with the indicated probability.

Matsui's Use of Constraints

Rounds	Equation	Pr	Equations Used
3	$P_L[3,8,14,25] \oplus P_R[17] \oplus C_L[3,8,14,25] \oplus C_R[17]=K_1[26] \oplus K_3[26]$	$½+1.56x2^{-3}$	A-A
5	$P_L[17] \oplus P_R[1,2,4,5,3,8,14,25] \oplus C_L[17] \oplus C_R[1,2,4,5,3,8,14,25]=K_1[2,3,5,6] \oplus K_2[26] \oplus K_4[26] \oplus K_5[2,3,5,6]$	$½+1.22x2^{-6}$	BA-AB
15	$P_L[8,14,25] \oplus P_R[16,20] \oplus C_L[3,8,14,25] \oplus C_R[17]=K_1[9,13] \oplus K_3[26] \oplus K_4[26] \oplus K_5[26] \oplus K_7[26] \oplus K_8[26] \oplus K_9[26] \oplus K_{11}[26] \oplus K_{12}[26] \oplus K_{13}[26] \oplus K_{15}[26]$	$½+1.19x2^{-22}$	E-DCA-ACD-DCA-A
16	$P_L[8,14,25] \oplus P_R[16,20] \oplus C_L[17] \oplus C_R[1,2,4,5,3,8,14,25]=K_1[9,13] \oplus K_3[26] \oplus K_4[26] \oplus K_5[26] \oplus K_7[26] \oplus K_8[26] \oplus K_9[26] \oplus K_{11}[26] \oplus K_{12}[26] \oplus K_{13}[26] \oplus K_{15}[26] \oplus K_{16}[2,3,5,6]$	$½-1.49x2^{-24}$	E-DCA-ACD-DCA-AB

Linear Cryptanalysis of full DES

Can be accomplished with ~2^{47} known plaintexts

- Using a slightly more sophisticated estimation 15 round approximation (with 2^{47} work factor)
  - For each 48 bit last round subkey, decrypt ciphertext backwards across last round for all sample ciphertexts
  - Increment count for all subkeys whose linear expression holds true to the penultimate round
  - This is done for the first and last round yielding 7 key bits each (total: 14)

Linear Cryptanalysis of full DES

- Can be accomplished with $\sim 2^{43}$ known plaintexts, using a more sophisticated estimation 14 round approximation
  - For each 48 bit last round subkey, decrypt ciphertext backwards across last round for all sample ciphertexts
  - Increment count for all subkeys whose linear expression holds true to the penultimate round
  - This is done for the first and last round yielding 13 key bits each (total: 26)

- Here they are:

  $P_R[8,14,25] \oplus C_L[3,8,14,25] \oplus C_R[17] = K_1[26] \oplus K_3[4] \oplus K_4[26] \oplus K_6[26] \oplus K_7[4] \oplus K_8[26] \oplus K_{10}[26] \oplus K_{11}[4] \oplus K_{12}[26] \oplus K_{14}[26]$

  with probability $\frac{1}{2} - 1.19 \times 2^{-21}$

  $C_R[8,14,25] \oplus P_L[3,8,14,25] \oplus P_R[17] = K_{13}[26] \oplus K_{12}[24] \oplus K_{11}[26] \oplus K_9[26] \oplus K_8[24] \oplus K_7[26] \oplus K_5[26] \oplus K_4[4] \oplus K_3[26] \oplus K_1[26]$

  with probability $\frac{1}{2} - 1.19 \times 2^{-21}$

Block Cipher Modes of Operation

- ECB: $y_i = E_K(x_i)$,
- CBC: $y_0 = IV$, $y_i = E_K(x_i \oplus y_{i-1})$.
- OFB: $z_0 = IV$, $z_{i+1} = E_K(z_i)$, $y_i = x_i \oplus z_i$.
- CFB: $y_0 = IV$, $z_i = E_K(y_{i-1})$, $y_i = x_i \oplus z_I$
- CTR: $x_j = x_{j-1}+1$, $o_j = L8(E_K(x_{j-1}))$, $c_j = x_j \oplus o_j$

Avoid ECB since it leaks too much information

Review: Arithmetic of $GF(2^n)$

- Suppose m(x) is an irreducible polynomial of degree n over GF(2): $m(x)= x^n + m_{n-1} x^{n-1} + \ldots + m_{0.}$
- Let a(x) and b(x) be polynomials of degree <n. They form a vector space of dimension n over GF(2). Coefficients of like exponent "add": $(a_{n-1} x^{n-1} + \ldots + a_0)+ (b_{n-1} x^{n-1} + \ldots + b_0)= (a_{n-1}+ b_{n-1})x^{n-1} + \ldots + a_0 + b_0)$
- Euclidean algorithm: for a(x), b(x) polynomials of degrees $m \leqq n$, there are polynomials q(x), r(x), deg r(x) <n such that a(x)=q(x)b(x)+r(x)
- Polynomials over GF(2) modulo m(x) form a field (with 2^n elements). Multiplication is multiplication of polynomials mod m(x).
- Inverses exist : If a(x) and b(x) are polynomials their greatest common denominator d(x) can be written as

  d(x)= a(x)u(x)+b(x)v(x) for some u(x), v(x).

In particular if a(x) and b(x) are co-prime: 1= a(x)u(x)+b(x)v(x) for some u(x), v(x).

Example of multiplication and inverse

- $m(x)= x^2 +x +1$. $m(x)$ is irreducible (otherwise it would have a root in GF(2)
- $x+(x+1) =1$, $1+(x+1)= x$
- $(x+1)(x+1)= x^2+2x+1=x^2+1= (x) + (x^2 +x +1)= x \pmod{m(x)}$
- $(x+1)$ and $m(x)$ are co-prime in fact,

  $1= (x+1) (x) + (x^2 +x +1)(1)$
- So "x" is the multiplicative inverse of "x+1" in GF(4).
- Usually elements of GF(2^n) are written in place notation so $x^5+x^3 +x^2 +1= 101101$.

End