University of Washington
CSEP 590TU – Practical Aspects of Modern Cryptography

Instructors: Josh Benaloh, Brian LaMacchia, John Manferdelli

Tuesdays: 6:30-9:30, Allen Center 305
Webpage: http://www.cs.washington.edu/education/courses/csep590/06wi/
Recommended texts:


Ferguson and Schneier, Practical Cryptography.
## New Lecture Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Lecturer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/3 Practical Aspects of Cryptography</td>
<td>Josh</td>
</tr>
<tr>
<td>2</td>
<td>1/10 Symmetric Key Ciphers and Hashes</td>
<td>John</td>
</tr>
<tr>
<td>3</td>
<td>1/17 Public Key Ciphers</td>
<td>Josh</td>
</tr>
<tr>
<td>4</td>
<td>1/24 Cryptographic Protocols I</td>
<td>Brian</td>
</tr>
<tr>
<td>5</td>
<td>1/31 Cryptographic Protocols II</td>
<td>Brian</td>
</tr>
<tr>
<td>6</td>
<td>2/7 Security of Block Ciphers</td>
<td>John</td>
</tr>
<tr>
<td>7</td>
<td>2/14 AES and Cryptographic Hashes</td>
<td>John</td>
</tr>
<tr>
<td>8</td>
<td>2/21 Trust, PKI, Key Management [Last HW Assignment]</td>
<td>Brian</td>
</tr>
<tr>
<td>9</td>
<td>3/1 Random Numbers/Elliptic Curve Crypto</td>
<td>Josh</td>
</tr>
<tr>
<td>10</td>
<td>3/8 Three topics: Elections, ITAR/Politics, Side Channels/Timing Attacks, DRM, BigNum Implementation</td>
<td>All</td>
</tr>
</tbody>
</table>
Analysis of Block Ciphers

John Manferdelli
jlms@cs.washington.edu
jmanfer@microsoft.com


This material is provided without warranty of any kind including, without limitation, warranty of non-infringement or suitability for any purpose. This material is not guaranteed to be error free and is intended for instructional use only.
Digital Block Ciphers

Complicated keyed invertible functions constructed from iterated elementary rounds.
  • Confusion: non-linear functions (ROM lookup)
  • Diffusion: permute round output bits
  • Key mixing: xor “key schedule” at beginning of round

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

DES (1974) design was watershed in public symmetric key crypto.
Iterated Feistel Cipher

Key Schedule

Key

Plaintext

Ciphertext

\[ \text{r Feistel Rounds} \]

\[ k_1, k_2, k_r \]
Figure 5.1. Electronic Codebook (ECB) Mode—Enciphering Computation.
Figure 5.2. Electronic Codebook (ECB) Mode—Calculation of \( f(R,K) \).

- \( E \) = E function
- KS = Key Schedule
- \( K_n \) = Changes for \( n=1, 2, \ldots, 16 \)
Figure 5.3. Electronic Codebook (ECB) Mode—Key Schedule (KS) Calculation.
DES Attacks: Exhaustive Search

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

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

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

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:

\[ \text{DES}_K(x) = IP^{-1} \sigma_{16} \tau \ldots \sigma_3 \tau \sigma_2 \tau \sigma_1 IP(x) \]

So its inverse is

\[ \text{DES}_K^{-1}(x) = IP^{-1} \sigma_1 \tau \ldots \sigma_{14} \tau \sigma_{15} \tau \sigma_{16} IP(x) \]

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: If \( a \) and \( b \) are chosen at random from \( S_n \) there is a good chance that \( <a, b> = A_n \) or \( S_n \).
DES Key Schedule

\[ C_0D_0 = \text{PC}_1(K) \]
\[ C_{i+1} = \text{LeftShift}(\text{Shift}_i, C_i), \quad D_{i+1} = \text{LeftShift}(\text{Shift}_i, D_i), \]
\[ K_i = \text{PC}_2(C_i \ || D_i) \]

\[ \text{Shift}_i = <1,2,2,2,2,2,2,1,2,2,2,2,2,2,1,1> \]

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 $E_{k_1}(E_{k_2}(m)) = m$.
  – 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 $DES_K(DES_K(x)) = x$. 
Birthday Attacks

- Probability of collision determined by “Birthday Paradox” calculation:
  - \((1-1/n)(1-2/n) \ldots (1-(k-1)/n)= (n!/k!)/n^k\)
  - Probability of collision is > .5 when \(k^2 > n\).
  - \(1+x \leq e^x, \prod_{i=1}^{i=k} (1-i/n) \leq e^{-k(k-1)/(2n)}\)
Meet in the Middle

Does double encryption double effective key size? Suppose:
\[ E'_{(a,b)}(p) = E_b(E_a(p)) \]

Attack if DES is a group. [\( E_k(p) = E_b(E_a(p)) \)].
But it isn’t: Campbell and Weiner, DES is not a Group, Crypto ’92.

Time Memory tradeoff [Known plaintext \((p_1, c_1), (p_2, c_2)\)]
Store \( E_a(p) = x \), Calculate \( E^{-1}_b(c) = y \).
The Linear Attack (Full Monty)

• Suppose $\Lambda$ is a cipher, the ciphertext and plaintext both come from $\text{GF}(2)^n$, $c=Kp$, where $K$ is an $n \times n$ invertible matrix, $K=(k_{ij})$ over $\text{GF}(2)$. How can we “break” $\Lambda$?

• Answer: Get (about) $n$ corresponding plaintext-ciphertext pairs $(p_i, c_i)$. Solve resulting linear equations to invert $K$. 
The Linear Attack (Partial Monty)

Suppose $L$ is a cipher, the ciphertext and plaintext both come from $GF(2)^n$, with key bits $k_i$, $i = 1, 2, \ldots, n$. How can we "break" $L$?

Answer: Obtain $m$ (linearly independent) linear relations

- $F_i(c) + G_i(p) = a_{i_1} k_1 + \ldots + a_{i_m} k_m$, $i = 1, 2, \ldots, m$
- Guess $n - m - 1$ bits of the key, solve for the other $m$ bits
- Time: $2^{n-m-1} + O(m)$ vs $2^n$
- Much faster than exhaustive search $O(2^n)$
Almost True Linear Constraints

• Usually finding linear relations is hard or impossible
• Look for linear relations that hold with probability \( p > 1/2 \)
• Collect a number of samples
• Vote for the maximally consistent subset of equations
• Suppose you have \( n \) (linear) equations hold with probability \( p \), what is the probability of \( m \) of them being correct.
  \[ \binom{n}{m} p^m (1-p)^{n-m} \]
• Large consistent subsets very likely to be correct even if \( p \) is only slightly bigger than .5
Almost Linear Attacks

- Sparse Representation
- Decomposition
- Transformation
- “Almost Linear” constraints
- Differential Cryptanalysis
- Linear Cryptanalysis
Algebraic Representations

- **Algebraic normal form (ANF):**

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

- **Degree:** \(\text{deg}(f)\), the highest degree term in ANF.
  - Example
    - \(f(X) = x_1 + x_2\), \(\text{deg}(f)=1\)
    - \(g(X) = x_1 x_2\), \(\text{deg}(g)=2\)

- Functions of degree 1 are called “affine”. Composition of Affine functions is affine.

- Lagrange Interpolation Theorem. Every function in \(n\) variables can be expressed as a polynomial (hence ANF).
Boolean Functions

- For a set of Boolean functions $\Delta$, $d(f,g)=\#\{X|f(X) \neq g(X)\}$.
- **Distance**: For Boolean function $f(X)$ and $g(X)$, $d(f,\Delta) = \min_{g(X) \in \Delta} d(f,g)$
- **Affine function**: $h(x) = a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n + c$
- $nl(f)$ denotes the minimum distance between $f(X)$ and the set of affine functions $\Delta_{affine}$. $nl(f) = d(f, \Delta_{affine})$, $\Delta_{affine} = RM(1,n)$.
- **Balance**: $f(X)$ is balanced iff there is an equal number of 0’s and 1’s in the output of $f(X)$.
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+1
356+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+125
6+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

\[ E_{k_1\|k_2}(x) = E'_{k_1}(x) \parallel E''_{k_2}(x) \]

\[
\begin{array}{|c|c|c|c|}
\hline
m & t & 2^{mt} & m2^t \\
\hline
2 & 32 & 2^{64} & 2^{33} \\
\hline
4 & 16 & 2^{64} & 2^{18} \\
\hline
\end{array}
\]
Linear Attacks on sparse coefficients

\[ c_1 = f[1,0](k_1,\ldots,k_m) p_1^0 p_2^0 \ldots p_n^0 + f[1,1](k_1,\ldots,k_m) p_1^1 p_2^0 \ldots p_n^0 + \ldots + f[1,2^m](k_1,\ldots,k_m) p_1 p_2 \ldots p_n \]

\[ \vdots \quad \vdots \quad \vdots \]

\[ c_n = f[n,1](k_1,\ldots,k_m) p_1 p_2 \ldots p_n + f[1,1](k_1,\ldots,k_m) p_1^1 p_2^0 \ldots p_n^0 + \ldots + f[1,2^m](k_1,\ldots,k_m) p_1 p_2 \ldots p_n \]

Suppose most of the \( f[i,j] \) are 0. Can solve for these with different \( p_1, p_2, \ldots, p_n \), even if the \( F[i,j] \) are complex and non-linear in the \( k_1,\ldots,k_m \).
Mathematics of Boolean Functions

• Correlation
  – \( c(f,g) = P[f(x)=g(x)] - P[f(x) \neq g(x)] \). So
    \[ P[f(x)=g(x)] = 0.5(1+c(f,g)) \]

• Hadamard
  – \( S_f(w) = 2^{-n} \sum_x (-1)^{f(x)+w \cdot x} = c(f(x), w x) \)

• Bent functions
  Furthest from linear (all Hadamard coefficients are equal)
Differential Cryptanalysis of Biham and Shamir (1990)

- Was known to IBM team whose design rules provided some resistance
- Breaks Khafre with 1500 corresponding plain/cipher texts in an hour
- Breaks 8 round Lucifer in $2^{21}$ steps with 24 texts
- Breaks FEAL.
- Breaks 8 round DES.
- Useful in breaking cryptographic hashes
- DES Results: $2^{47}$ Chosen plaintext attack.
Differential Cryptanalysis: Overview

Let \((P_L, P_R), (P_L^*, P_R^*)\) and \((C_L^*, C_R^*), (C_L^*, C_R^*)\) be pairs of inputs and outputs with prescribed xors

\[
(P_L', P_R') = (P_L, P_R) \oplus (P_L^*, P_R^*)
\]
\[
(C_L', C_R') = (C_L, C_R) \oplus (C_L^*, C_R^*)
\]

Follow the xor of two plaintexts through rounds of DES. Output xor depends non uniformly on key bits. Take lots of chosen plaintext/ciphertext pairs. Let non uniform distribution “vote” on set containing keys.
Consider a round of DES: $\sigma_K: (L,R) \rightarrow (L \oplus F(E(R) \oplus K), R)$ where if $X=X_1 || X_2 || \ldots || X_8$ with each $X_i$ a six bit quantity.

$F(X) = P(S_1(X_1) || \ldots || S_8(X_8))$

Let $(L, R)$ and $(L^*, R^*)$ be inputs to a round of DES and

$(L', R') = (L, R) \oplus (L^*, R^*)$.

At each S-box position, an input xor is independent of key and the distribution of the output xors is very non-linear and not all output xors are possible. Keys choose among output xors. Aside from S-box, all operations are linear.
Differential Profile of single S-box

- If \( x' \rightarrow y' \) and \( D_j(x', y') = \{ u : S_j(u \oplus x') \oplus S_j(u) = y' \} \), then \( k \in x \oplus D_j(x', y') \).
- \( |D_j(x', y')| \) has non uniform distribution.
- The propagation ratio, \( R_p(x', y') = |D_j(x', y')| / 2^m \), where \( m \) is the dimension of the space of \( a' \).
  - Shamir and Biham denote this as \( x' \rightarrow y', p \).
    \( (p = |D_j(x', y')| / 2^m) \).
S1 Differential Distribution

S box 1

<table>
<thead>
<tr>
<th>In</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>64</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>10</td>
<td>12</td>
<td>4</td>
<td>10</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>6</td>
<td>8</td>
<td>6</td>
<td>12</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>14</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>10</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>8</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>12</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>6</td>
<td>2</td>
<td>8</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>4</td>
<td>10</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>0</td>
<td>8</td>
<td>8</td>
<td>4</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>8</td>
<td>8</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>8</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>a</td>
<td>0</td>
<td>8</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>8</td>
<td>6</td>
<td>0</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>b</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>10</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>c</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>d</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>8</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>6</td>
<td>0</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>e</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>8</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>f</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>14</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>12</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>
S box 1
In  0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f

13  2  4  4  6  2  0  4  6  2  0  6  8  4  6  4  6
14  0  8  8  0 10  0  4  2  8  2  2  4  4  8  4  0
15  0  4  6  4  2  2  4 10  6  2  0 10  0  4  6  4
16  0  8 10  8  0  2  2  6 10  2  0  2  0  6  2  6
17  4  4  6  0 10  6  0  2  4  4  4  6  6  6  6  2  0
18  0  6  6  0  8  4  2  2  2  4  6  8  6  6  6  2  2
19  2  6  2  4  0  8  4  6 10  4  0  4  2  8  4  0
1a  0  6  4  0  4  6  6  6  6  2  2  0  4  4  6  8
1b  4  4  2  4 10  6  6  4  6  2  2  4  2  2  4  2
1c  0 10 10  6  6  0  0 12  6  4  0  0  2  4  4  0
1d  4  2  4  0  8  0  0  2 10  0  2  6  6  6 14  0
1e  0  2  6  0 14  2  0  0  6  4 10  8  2  2  6  2
1f  2  4 10  6  2  2  2  8  6  8  0  0  0  4  6  4
20  0  0  0 10  0 12  8  2  0  6  4  4  4  2  0 12
21  0  4  2  4  4  8 10  0  4  4 10  0  4  0  2  8
22 10  4  6  2  2  8  2  2  2  6  0  4  0  4 10
23  0  4  4  8  0  2  6  0  6  6  2 10  2  4  0 10
24 12  0  0  2  2  2  2  0 14 14  2  0  2  6  2  4
S box 1

In  0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
25  6  4  4  12  4  4  4  10  2  2  2  0  4  2  2  2
26  0  0  4  10  10  10  2  4  0  4  6  4  4  4  2  0
27  10  4  2  0  2  4  2  0  4  8  0  4  8  8  4  4
28  12  2  2  8  2  6  12  0  0  2  6  0  4  0  6  2
29  4  2  2  10  0  2  4  0  0  14  10  2  4  6  0  4
2a  4  2  4  6  0  2  8  2  2  14  2  6  2  6  2  2
2b 12  2  2  2  4  6  6  2  0  2  6  2  6  0  8  4
2c  4  2  2  4  0  2  10  4  2  2  4  8  8  4  2  6
2d  6  2  6  2  8  4  4  4  2  4  6  0  8  2  0  6
2e  6  6  2  2  0  2  4  6  4  0  6  2  12  2  6  4
2f  2  2  2  2  6  8  8  2  4  4  6  8  2  4  2
30  0  4  6  0  12  6  2  2  8  2  4  4  6  2  2  4
31  4  8  2  10  2  2  2  2  6  0  0  2  2  4  10  8
32  4  2  6  4  4  2  2  4  6  6  4  8  2  2  8  0
33  4  4  6  2  10  8  4  2  4  0  2  2  4  6  2  4
34  0  8  16  6  2  0  0  12  6  0  0  0  0  8  0  6
35  2  2  4  0  8  0  0  0  14  4  6  8  0  2  14  0
36  2  6  2  2  8  0  2  2  4  2  6  8  6  4  10  0
### S1 Differential Distribution

**S box 1**

<table>
<thead>
<tr>
<th>In</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>2</td>
<td>2</td>
<td>12</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>10</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>38</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>39</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>12</td>
<td>6</td>
<td>4</td>
<td>8</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>3a</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3b</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>3c</td>
<td>0</td>
<td>10</td>
<td>4</td>
<td>0</td>
<td>12</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>12</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3d</td>
<td>0</td>
<td>8</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>0</td>
<td>8</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>12</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3e</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>14</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>8</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3f</td>
<td>4</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>8</td>
<td>6</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Example: Differential Cryptanalysis of S1 through a single round

\[ S_{1E} = 0x01, \quad S_{1E} = 0x35 \rightarrow 0x0d = S_O'. \]
\[ S_{1E} = 0x21, \quad S_{1E} = 0x15 \rightarrow 0x03 = S_O'. \]

0x34 \rightarrow 0x0d means input difference 0x34 produced output difference 0x0d

(1) For 0x34 \rightarrow 0xd, \( S_1' = \{0x06, 0x10, 0x16, 0x1c, 0x22, 0x24, 0x28, 0x32\} \).

(2) For 0x34 \rightarrow 0x3, \( S_1' = \{0x01, 0x02, 0x15, 0x21, 0x35, 0x36\} \).

Since \( S_{1E} + S_1 = S_1K \),

(1) Reduces the possible key set to \{0x07, 0x33, 0x11, 0x25, 0x17, 0x23, 0x1d, 0x29\}

(2) Reduces the possible key set to \{0x20, 0x14, 0x23, 0x17, 0x34, 0x00\}.

The intersection (and actual possibilities) are \{0x17, 0x23\}
One Round Differential used to analyze 4 round DES

Method

Use 1 round characteristic to right. Undo effect of permutation matrix and solve each S box separately. This allows us to solve for 48 key bits. This 1 round characteristic will be used to estimate input xor in subsequent rounds.
Differential Cryptanalysis of 4 rounds

Because $b' = L_0'$, the output xor of $S_2, S_3, \ldots, S_8$ in round 2 is 0. This gives 28 bits of $B'$ and hence 28 bits of $D'$ is known.

Since $B'$ is known, we can calculate $D' = B' \oplus L_4'$ using 4 encrypted pairs for each of the 7 relevant $S$ boxes. All key candidates are in this set which gives $7 \times 6 = 42$ bits of key with high probability.
A *one round characteristic* is a triple

\[ \left( \left( L_{in} ', R_{in} ' \right), \left( L_{out} ', R_{out} ' \right), p \right) \]

such that for all pairs \((L_{in}, R_{in}), (L_{in} *, R_{in} *)\) with

\[ \left( L_{in}, R_{in} \right) \oplus \left( L_{in} *, R_{in} * \right) = \left( L_{in} ', R_{in} ' \right) \]

subjected to a single cipher round (depicted on the right) producing corresponding pairs \((L_{out}, R_{out}), (L_{out} *, R_{out} *)\), the ratio of output pairs with \((L_{out}, R_{out}) \oplus (L_{out} *, R_{out} *) = (L_{out} ', R_{out} ')\) is \(p\).

Characteristics can be extended through multiple rounds.
Computing a single characteristic

- The first and most important differential is \((L',0) \rightarrow (L',0)\), \(p=1\).
- Another is \((L',0x60000000) \rightarrow (L' \oplus 0x00808200,0x60000000)\), \(p=1/4\).
- Construction:
  - \(E(0x60000000)= E(0110 0000 \ldots 0000)= 001100 000000 \ldots 000000\)
  - \(S_1(001100)' \rightarrow 0xe\) with \(p=1/4\), \(S_j(0)' \rightarrow 0\) with \(p=1\), \(j>1\) and \(P(0xe0000000)=0x00808200\).
Multi-round Characteristics

- Sequence of Differentials with identified input and output xors. Each round differential occurs with probability $p_i$.
- Overall probability: $p = \prod p_i$
- Characteristic to the right is a three round characteristic with probability $\left(\frac{14}{64}\right)^2$
- Used to approximate differentials through multiple rounds.
- Each pair following the characteristic at each round is called a "right pair". Other pairs are "wrong pairs."
- Wrong pairs get distributed uniformly; right pairs follow overall characteristic probability.

\[
\Omega_p = 00 \ 80 \ 82 \ 00 \ 60 \ 00 \ 00 \ 00 \\
A' = 00 \ 80 \ 82 \ 00 \ a' = 60 \ 00 \ 00 \ 00 \ p = 14/64 \\
B' = 0 \ b' = 0 \ p = 1 \\
C' = 00 \ 80 \ 82 \ 00 \ c' = 60 \ 00 \ 00 \ 00 \ p = 14/64 \\
\Omega_c = 00 \ 80 \ 82 \ 00 \ 60 \ 00 \ 00 \ 00
\]
Multi-round Characteristics - Formal

- An n-round characteristic is a triple \((\Omega_p, \Lambda, \Omega_T)\), with \(\Lambda=(\Lambda_1, \ldots, \Lambda_n)\) where each \(\Lambda_1\) is a one round differential that holds with probability \(p_i\), with first round input xor (to \(\Lambda_1\)) is \(\Omega_p\), and last round output xor (form \(\Lambda_n\)) is \(\Omega_T\) and rounds “match up”.

- Probability of combined n-round characteristic is \(p^\Omega=\prod p_i\)

- Each pair following the characteristic at each round is called a “right pair”. Other pairs are “wrong pairs.”

- Wrong pairs get distributed uniformly; right pairs follow overall characteristic probability.
Constructing 3 Round Characteristic

- Use
- \((L',0) \rightarrow (L',0), \ p=1\).
- \((0x00808200, 0x60000000) \rightarrow (0x00808200, 0x60000000), \ p=1/4\).
Two round iterative characteristic

- \( p = \frac{1}{234} \)
- Obviously useful for multi-round estimates
Differential Cryptanalysis of 3 Round DES

\[ R_3 = L_2 + f(E(R_2) + k_2) \]
\[ = R_1 + f(E(R_2) + k_2) \]
\[ = L_0 + f(E(R_0) + k_1) + f(E(R_2) + k_3) \]

Pick pair \((R_0, R_0^*)\) with
\[ R_0 + R_0^* = R_0' = 0. \]

\[ R_3' + L_0' = f(E(R_2) + k_3) + f(E(R_2^*) + k_3) \]

\[ P^{-1}(R_3' + L_1') = f(E(R_2) + k_3) + f(E(R_2^*) + k_3) \]

Note \(R_2 = L_3\).
Data for Differential Cryptanalysis of 3 Round DES

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x748502cd38451097</td>
<td>0x03c70306d8a09f10</td>
</tr>
<tr>
<td>0x3874756438451097</td>
<td>0x78560a0960e6d4cb</td>
</tr>
<tr>
<td>0x486911026acdf31</td>
<td>0x45fa285be5adcc730</td>
</tr>
<tr>
<td>0x375bd31f6acdf31</td>
<td>0x134f7915ac253457</td>
</tr>
<tr>
<td>0x357418da013fec86</td>
<td>0xd8a31b2f28bbc5cf</td>
</tr>
<tr>
<td>0x12549847013fec86</td>
<td>0x0f317ac2b23cb944</td>
</tr>
</tbody>
</table>

Only one counter in each 6 bit set will be possible for all 3 pairs.
Three Round Characteristic

- This characteristic occurs with probability $p=1/16$ and forms an estimate for the differential input of the 4\textsuperscript{th} round of the 6 rounds.
- $(00 \ 20 \ 00 \ 08 \ 00 \ 00 \ 00 \ 04) \rightarrow (00 \ 00 \ 04 \ 00 \ 00 \ 20 \ 00 \ 08)$ with $p=1/16$ is another such characteristic.
Differential Cryptanalysis of 6 rounds

- Suppose \((L_{i-1}, R_{i-1}), k_i\) are the inputs to round \(i\). \(P_L = L_0, P_R = R_0\).
- \(L_6 = R_4 \oplus f(k_6, R_6) = L_3 \oplus f(k_6, R_6) \oplus f(k_4, R_3)\)
- \(L_6' = L_3' \oplus f(k_6, R_6) \oplus f(k_6, R_6') \oplus f(k_4, R_3) \oplus f(k_4, R_3')\)
- \(L_6' = C_L\) and \(R_6 = C_R\) are known.
- Estimate \(L_3' = 40000000, R_3' = 40080000\), using the differential.
- Set \(S = P^{-1}(C_L \oplus 40000000) = f(k_6, C_R) \oplus f(k_6, C_R') \oplus f(k_4, R_3) \oplus f(k_3, R_3') = S_1(E_1) || S_2(E_2) || ... || S_8(E_8)\) where \(E_1|| E_2|| ... || E_8\) are the bits obtained by applying \(E\) to 40080000.
- \(E_1|| E_2|| ... || E_8 = 00100000000000000101000...0 = 08||00||01||10||00||00||00||00.\)
- Since the input Xors to \(S_2, S_5, S_6, S_7, S_8\) are 0, \(f(k_4, R_3) \oplus f(k_4, R_3')\) is 0 in the corresponding output bit positions and we are left with the simple differential: \(P^{-1}(C_L \oplus 40000000) = f(k_6, C_R) \oplus f(k_6, C_R')\) for \(S_2, S_5, S_6, S_7, S_8\).
Differential Cryptanalysis of 6 rounds

• First characteristic yields 30 bits of key. Second one adds another 12 bits of key.
• Recall $P^{-1}(C_L \oplus 40000000) = f(k_6, C_R) \oplus f(k_6, C_R^*)$ for $S2, S5, S6, S7, S8$
• This occurs with $p = 1/16$.
• Straightforward implementation yielding 30 keybits:
  – Set up $2^{30}$ counters
  – Bump counter for suggested key for each pair of $n$ chosen texts
  – Correct key be will “voted” at least $1/16$ $n$ time (“right pairs”)
  – Incorrect keys will be voted randomly each with probability $1/2^{30}$
Differential Cryptanalysis of 6 rounds

- Improving the “signal to noise” ratio by “filtering” pairs
  - For each of S2, S5, S6, S7, S8 with input xor x’ and output xor y’, look at $x \oplus D_j(x',y')$.
  - If this is empty, this must be wrong pair.
  - For any given S box the, this happens with probability .2.
  - The probability that all 5 S boxes have non-empty candidate key sets is $(.8)^5=.33$. Call this set of pairs RP and the complement WP.
  - RP contains 1/3 of the pairs, WP contains 2/3.
  - In RP, the probability of a “correct vote” is 3/16.
“Signal to Noise”

- \( S/N = \frac{\text{right_pairs}}{\text{average_count}} \)
  - \( \alpha = \frac{\text{average_counted}}{\text{counted_pairs}} \)
  - \( \beta = \frac{\text{counted_to_all}}{} \)
  - \( m \) is the number of pairs

- \( S/N = \frac{mp}{(m \frac{\alpha \beta}{2^k})} = \frac{(2^k p)}{(\alpha \beta)} \)

- \( S/N \) affects number of right pairs needed:
  - \( S/N 1-2, 20-40 \) right pairs required
  - \( S/N 16, 7-8 \) right pairs required
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 $\sqrt{2m} \times 2^{32}$ are required for corresponding plaintext
Comments on Differential Cryptanalysis of full DES

<table>
<thead>
<tr>
<th># Rounds</th>
<th>Needed pairs</th>
<th>Analyzed Pairs</th>
<th>Bits Found</th>
<th># Char rounds</th>
<th>Char prob</th>
<th>S/N</th>
<th>Chosen Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$2^3$</td>
<td>$2^3$</td>
<td>42</td>
<td>1</td>
<td>1</td>
<td>16</td>
<td>$2^4$</td>
</tr>
<tr>
<td>6</td>
<td>$2^7$</td>
<td>$2^7$</td>
<td>30</td>
<td>3</td>
<td>1/16</td>
<td>$2^{16}$</td>
<td>$2^8$</td>
</tr>
<tr>
<td>8</td>
<td>$2^{15}$</td>
<td>$2^{13}$</td>
<td>30</td>
<td>5</td>
<td>1/1048</td>
<td>15.6</td>
<td>$2^{16}$</td>
</tr>
<tr>
<td>16</td>
<td>$2^{57}$</td>
<td>$2^5$</td>
<td>18</td>
<td>15</td>
<td>$2^{-55.1}$</td>
<td>16</td>
<td>$2^{58}$</td>
</tr>
</tbody>
</table>
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.
- \( S(X) \neq S(X \oplus 001100) \) differ in at least 2 bits.
Comments on effect of components on Differential Cryptanalysis

• E
  – Without expansion, there is a 4 round iterative characteristic with $p = \frac{1}{256}$

• 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 $p = \frac{1}{73}$. 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 $\gamma_i$, linear, for $i = 1,2,\ldots,m$.

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 $\gamma$, 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). $\epsilon$ is called “bias”.

Breaks 16 round DES with $2^{47}$ work factor (actually a little more complicated than simple voting over whole cipher).
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:

\[ M(i) = 64 - EE(i). \]

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 $NS_5(010000,1111)= 12$:

$$X[2] \oplus Y[1,2,3,4]=K[2] \oplus 1,$$


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:
Thus holds with \( p = (52/64)^2 + (12/64)^2 = .66 \)
Matsui’s Per Round Constraints

<table>
<thead>
<tr>
<th>Label</th>
<th>Equation</th>
<th>Pr</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>$X[1,2,4,5] \oplus Y[17]=K[2,3,5,6]$</td>
<td>22/64</td>
</tr>
</tbody>
</table>

Matsui: Linear Cryptanalysis Method for DES Cipher. Eurocrypt, 98.
Linear Cryptanalysis of 5 rounds

Pattern: BA-AB.

\[ P_L[17] \oplus R_1[17] \oplus P_R[1,2,4,5] = k_1[2,3,4,5] \]
\[ L_1[3,8,14,25] \oplus R_2[3,8,14,25] \oplus R_1[17] = K_2[26] \]
\[ R_3[17] \oplus C_L[17] \oplus C_R[1,2,4,5] = K_5[2,3,5,6] \]

Adding yields

\[ P_L[17] \oplus P_R[1,2,4,5,3,8,14,25] \oplus C_L[17] \]
\[ \oplus C_R[1,2,4,5,3,8,14,25] = K_1[2,3,5,6] \oplus K_2[26] \]
\[ \oplus K_4[26] \oplus K_5[2,3,5,6] \]

\[ P = p_A^2 p_B^2 + (1-p_A)^2 p_B^2 + p_A^2 (1-p_B)^2 + (1-p_A)^2 (1-p_B)^2 + 4p_A p_B (1-p_A) (1-p_B) = 0.519 \]

JLM 20060209 12:16
Piling Up Lemma

Let $X_i$ ($1 \leq i \leq n$) 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

$$\frac{1}{2} + 2^{n-1} \prod_{[1,n]} (p_i - 1/2)$$

Proof:

By induction on $n$. It’s tautological for $n=1$.

Suppose $\Pr[X_1 \oplus X_2 \oplus ... \oplus X_{n-1} = 0] = q = \frac{1}{2} + 2^{n-2} \prod_{[1,n-1]} (p_i - 1/2)$. Then $\Pr[X_1 \oplus X_2 \oplus ... \oplus X_n = 0] = qp_n + (1-q)(1-p_n) = \frac{1}{2} + 2^{n-1} \prod_{[1,n]} (p_i - 1/2)$ as claimed.
Central Limit Theorem. Let $X, X_1, \ldots, X_n$ be independent, identically distributed random variables and let $S_n = X_1 + X_2 + \ldots + X_n$. Let $\mu = E(X)$ and $\sigma^2 = E((X-\mu)^2)$. 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

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

$n$ is called the Normal Distribution and is symmetric around $x=0$. $N(-\infty,0) = \frac{1}{2}$. $N(-.5,.5) = .38$, $N(-.75,.75) = .55$, $N(-1,1) = .68$, $N(-2,2) = .9546$, $N(-3,3) = .9972$.
Application of CLT to LC

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 $Pr(T_n \geq -\varepsilon \sqrt{n/\sqrt{(1/4 - \varepsilon^2)}})$. If $n = \delta^2 \varepsilon^{-2}$, this is just $Pr(T_n \geq -\delta / \sqrt{(1/4 - \varepsilon^2)})$ or, if $\varepsilon$ is small $Pr(T_n \geq -2\delta)$.

Some numerical values: $\delta = .25$, $N(-.5, \infty) = .69$, $\delta = .5$, $N(-1, \infty) = .84$, $\delta = 1$, $N(-2, \infty) = .98$, $\delta = 1.5$, $N(-3, \infty) = .999$. 
15 Round Linear Approximation

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


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 Round Linear Approximation

Adding and canceling:

\[ \oplus K_9[26] \oplus K_{11}[26] \oplus K_{12}[4] \oplus K_{13}[26] \oplus K_{15}[26] \]

which holds (by Piling-up Lemma) with the indicated probability.
## Matsui’s Use of Constraints

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Equation</th>
<th>Pr</th>
<th>Equations Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$P_L[3,8,14,25] \oplus P_R[17] \oplus C_L[3,8,14,25] \oplus C_R[17] = K_1[26] \oplus K_3[26]$</td>
<td>$\frac{1}{2}+1.56 \times 10^{-3}$</td>
<td>A-A</td>
</tr>
<tr>
<td>5</td>
<td>$P_L[17] \oplus P_R[1,2,4,5,3,8,14,25] \oplus C_L[17] \oplus C_R[1,2,4,5,3,8,14,25] = K_1[2,3,5,6] \oplus K_2[26] \oplus K_4[26] \oplus K_5[2,3,5,6]$</td>
<td>$\frac{1}{2}+1.22 \times 10^{-6}$</td>
<td>BA-AB</td>
</tr>
<tr>
<td>16</td>
<td>$P_L[8,14,25] \oplus P_R[16,20] \oplus C_L[17] \oplus C_R[1,2,4,5,3,8,14,25] = K_1[9,13] \oplus K_3[26] \oplus K_4[26] \oplus K_5[26] \oplus K_7[26] \oplus K_8[26] \oplus K_9[26] \oplus K_{11}[26] \oplus K_{12}[26] \oplus K_{13}[26] \oplus K_{15}[26] \oplus K_{16}[2,3,5,6]$</td>
<td>$\frac{1}{2}-1.49 \times 10^{-24}$</td>
<td>E-DCA-ACD-DCA-AB</td>
</tr>
</tbody>
</table>
Framework for differentials and linear approximation

• Differentials
  - \((\Delta X_i, \Delta Y_i) = \Pr[F_i(X_i \oplus \Delta X_i, K_i) \oplus F_i(X_i, K_i) = \Delta Y_i]\)
  - \([p_1, p_2, ..., p_n] = \Pi p_i\)
  - \(B_i = \text{Max}(\{\Delta X_i = \Delta X_{i-2} \oplus \Delta Y_{i-1}, 3 \leq i \leq n\}) \ (\Delta X_1, \Delta Y_1) \ (\Delta X_2, \Delta Y_2) \ ... \ (\Delta X_n, Y_n)\)

• Linear Approximations
  - \((\Gamma X_i, \Gamma Y_i) = \Pr[\Gamma X \cdot X_i \oplus \Gamma Y \cdot F_i(X_i, K_i) = 0] - .5\)
  - \([p_1, p_2, ..., p_n] = 2^{t-1} \Pi p_i\)
  - \(B_i = \text{Max}(\{\Gamma Y_i = \Gamma Y_{i-2} \oplus \Delta \Gamma X_{i-1}, 3 \leq i \leq n\}) \ (\Gamma X_1, \Gamma Y_1) \ (\Gamma X_2, \Gamma Y_2) \ ... \ (\Gamma X_n, \Gamma Y_n)\)
Matsui’s algorithm for extending differentials and linear approximation

- Round -1
  Begin
  \[ p_1 = \max_{\Delta Y}( (\Delta X_1, \Delta Y) ) \]
  If \([p_1, B_{n-1}] > AB_n\), call Round-2
  End

- Round-2
  Begin
  \[ p_2 = \max_{\Delta X,\Delta Y}( (\Delta X_2, \Delta Y_2) ) \]
  If \([p_1, p_2, B_{n-2}] > AB_n\), call Round-3
  End

- Round –i (3 \leq i \leq n)
  Begin
  \[ \Delta X_i = \Delta X_{i-2} \oplus \Delta Y_{i-1} \]
  \[ p_i = \max_{\Delta Y}( (\Delta X_i, \Delta Y_i) ) \]
  If \([p_1, p_2, \ldots, p_i, B_{n-i}] > AB_n\), call Round-(i+1)
  End

- Round-n
  Begin
  \[ \Delta X_n = \Delta X_{n-2} \oplus \Delta Y_{n-1} \]
  \[ p_n = \max_{\Delta X,\Delta Y}( (\Delta X_n, \Delta Y) ) \]
  If \([p_1, p_2, \ldots, p_n] > AB_n\), then
  \[ AB_n = [p_1, p_2, \ldots, p_n] \]
  End
Linear Cryptanalysis of 8 rounds

7 Round approximation, $p^{-\frac{1}{2}} = 1.95 \times 2^{-10}$


$C_L = C_L' \oplus F(C_R',K_8)$

$C_R = C_L'$
Linear Cryptanalysis of full DES

Can be accomplished with $\sim 2^{47}$ 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:


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


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

- DesX fixes two critical problems with DES:
  - Key size is too small
  - Practical Linear and Differential attacks rely on access to first and last rounds of iterated cipher
- DesX replaces the 56 bit DES key, k with a 184 bit key \((k_i, k, k_o)\)
- \(\text{DESX}(k_i, k, k_o; x) = k_o \oplus \text{DES}_k(x \oplus k_i)\)
- Xoring key bits at input and output of cipher is called “whitening” and is used extensively by AES candidates
- DESX was proposed by Rivest and doesn’t adversely affect the encryption/decryption speed
Brute Force Known-Plaintext Attacks on DES

- There are $2^{56} = \text{about } 7.2 \times 10^{16}$ possible keys
  - about 72 thousand trillion
- Diffie and Hellman - 1976
  - a $20\text{ M}$ machine with 1-million processors, each capable of testing 1 M DES keys/sec, could search $10^{12}$ keys/sec and all keys in a day.
- Michael Wiener - 1993
  - $1\text{ M}$ machine with 57,600 search chips, each testing 50 M keys/s, could break in 3.5 hours on average.
- EFF
  - 7/13/98, $10\text{K}$ RSA prize awarded to EFF which broke DES with $210\text{K}$ machine.
DES Attacks

- Differential cryptanalysis: This attack requires the encryption of $2^{47}$ chosen plaintexts.
- Linear cryptanalysis. By means of this method, a DES key can be recovered by the analysis of $2^{43}$ known plaintexts.
- First Aid: use 3-DES or DES-X: $\text{DESX}(k_1,k_2,k_3,x) = k_2 \oplus \text{DES}(k_1,x \oplus k_3)$
  - This “whitens” input and output.
Other attacks on DES

- Multiple Linear Approximations, Knudsen & Robshaw
- Related Keys, Biham
  - Introduce controlled diffusion producing predictable effect that depends on related keys. Also applies to hash functions.
  - Applies to LOKI and Lucifer but not DES (because of irregular key selection schedule)
- Non-Linear Approximations, Knudsen and Robshaw
  Hard to knit constraints together, some help on first and last rounds
- Davies Attack, improved by Biham and Biryukov
  Output on adjacent S-boxes share keys and parity of non-shared keys have non-uniform distributions. Marginally better than exhaustive search
- Boomerang Attack, Slide attack, Wagner.
Triple-DES

Part of FIPS 46-3 standard
Encrypt: $C = E(K_3, D(K_2, E(K_1, P)))$
Decrypt: $P = D(K_3, E(K_2, D(K_1, C))$)

3-key: $K_1$, $K_2$, $K_3$ all different
   get 168-bit key
2-key: $K_1 = K_3$ (Two key version is subject to a time-memory trade-off attack)
   get 112-bit key
   better than double encryption
Post DES Design Criteria

• Use inverses in $\text{GF}(2^k)$. ($k=8$ is popular) – Mars, Rijndael
• S-Boxes should be surjective
• If S-Boxes define permutations ($\pi$),
  - $\text{DP}_{\text{max}}(\pi) = \max_{\{a \neq 0, b\}} \Pr(\pi(x \oplus a) \oplus \pi(x) = b) < 10/256$
  - $\text{LP}_{\text{max}}(\pi) = (2\Pr(x \cdot a = \pi(a) \cdot b) - 1)^2 < 1/16$
  - Few Fixed points (3 for 256)
DES Summary

• DES was a great cipher.
• They should have stuck with a 64-bit key.
  – More secure
  – Better as a Hash primitive
• To make DES better.
  – Increase key size!
  – Pre and post whitening and non-key based mixing
  – Calculate differentials and dependencies and make them small enough so not enough plain/cipher is available for linear and differential attacks.
Homework 6 – Problem 1

S-box 4 is observed to have the indicated output xor when presented with the indicated inputs

In1: 0x22, In2: 0x16, Output xor: 0x0c
In1: 0x12, In2: 0x0c, Output xor: 0x05

Perform a differential cryptanalysis and produce the possible candidate key(s). You may find the tables provided in “DC.txt” helpful.
Homework 6, problem 2 (omit)

Consider the 2 round iterative differential characteristic for DES
0x19600000000000 → 0x19600000000000, p=1/234

Suppose for the following questions we can always find chosen plaintext with S/N ratio high enough to require only 10 “right pairs” for a successful differential cryptanalysis (“DC”).

a. On average, how many chosen plain ciphertext pairs are required for a successful DC on two rounds?

b. On average, how many chosen plain ciphertext pairs are required for a successful DC on ten rounds?

c. After how many rounds is DC impossible because there cannot possibly be enough plain ciphertext pairs to succeed?
Homework 6 – Problem 3

A certain cipher $X$ with 6 bit key $k_1, k_2, k_3, k_4, k_5, k_6$ has 4 linear constraints.

Given the corresponding plaintext, ciphertext pairs and substituting the equations become:

\[
\begin{align*}
0 & = k_1 \oplus k_3 \oplus k_4 \\
0 & = k_4 \oplus k_5 \\
0 & = k_1 \oplus k_2 \\
1 & = k_1 \oplus k_6
\end{align*}
\]

Guessing $k_1$ and $k_3$ calculate $k_2$, $k_4$, $k_5$, $k_6$. How many encryptions are needed to discover the correct key with exhaustive search in the worst case?

How many are needed with these constraints?
Homework 6, problem 4

(A) Suppose the cipher \( C \) has a linear constraint (Equation 1) that holds with probability \( p = 0.75 \) where the input to \( X \) is plaintext bits \( i_1 \| i_2 \| \ldots \| i_6 \); the output is the ciphertext bits \( o_1 \| o_2 \| \ldots \| o_6 \) under key bits \( k_1 \| k_2 \| \ldots \| k_6 \). The constants \( a_1, a_2, \ldots, a_6, b_1, b_2, \ldots, b_6, c_1, c_2, \ldots, c_6, d \) are all known.

Equation 1: $$a_1 i_1 \oplus a_2 i_2 \oplus a_3 i_3 \oplus a_4 i_4 \oplus a_5 i_5 \oplus a_6 i_6 \oplus b_1 o_1 \oplus b_2 o_2 \oplus b_3 o_3 \oplus b_4 o_4 \oplus b_5 o_5 \oplus b_6 o_6 = c_1 k_1 \oplus c_2 k_2 \oplus c_3 k_3 \oplus c_4 k_4 \oplus c_5 k_5 \oplus c_6 k_6 \oplus d$$

Finally, suppose upon substituting values from 3 plaintext/ciphertext pairs the left hand side of equation 1 has values 1, 1, 0, respectively. What are the odds that \( c_1 k_1 \oplus c_2 k_2 \oplus c_3 k_3 \oplus c_4 k_4 \oplus c_5 k_5 \oplus c_6 k_6 \oplus d = 1 \) rather than 0?

(B) Suppose the same setup as in A but 3 out of 4 plaintext/ciphertext pairs "vote" that \( c_1 k_1 \oplus c_2 k_2 \oplus c_3 k_3 \oplus c_4 k_4 \oplus c_5 k_5 \oplus c_6 k_6 \oplus d = 1 \).

What are the odds that \( c_1 k_1 \oplus c_2 k_2 \oplus c_3 k_3 \oplus c_4 k_4 \oplus c_5 k_5 \oplus c_6 k_6 \oplus d = 1 \) rather than 0?
Homework 6, problem 4

(C) Constructing a multi-round constraint

Suppose $X$ is a four round iterative cipher with plaintext input, $P$ and ciphertext output $C$ where each round has 6 bit input $I$ and 6 bit output $O$ and per round keys $K^{(1)}, K^{(2)}, \ldots K^{(6)}$. Using Matsui’s notation suppose the contraints:

$I[1,2] \oplus O[3,4] = K^{(1)}[1,3]$ \hspace{1cm} \text{R1}
$I[3,4] \oplus O[1,5] = K^{(2)}[4,6]$ \hspace{1cm} \text{R2}
$I[1,5] \oplus O[1,6] = K^{(3)}[1,5]$ \hspace{1cm} \text{R3}
$I[1,6] \oplus O[2,5] = K^{(4)}[2]$ \hspace{1cm} \text{R4}

hold with probabilities $p_1 = .8$, $p_2 = .9$, $p_3 = .8$, $p_4 = .9$, respectively.

What is the probability that

$P[1,2] \oplus C[2,5] = K^{(1)}[1,3] \oplus K^{(2)}[4,6] \oplus K^{(3)}[1,5] \oplus K^{(4)}[2]$?
Homework 6, problem 4

(D) Suppose $X$ is a multi round iterative cipher with 40 bit plaintext input, $P$, and ciphertext output, $C$, and 40 bit key. Suppose, using Matsui’s notation, that the following four linearly independent constraints:

i. $P[a_1^{(1)}, a_2^{(1)}, ..., a_{40}^{(1)}] \oplus C[b_1^{(1)}, b_2^{(1)}, ..., b_{40}^{(1)}] = K[c_1^{(1)}, c_2^{(1)}, ..., c_{40}^{(1)}]$  
ii. $P[a_1^{(2)}, a_2^{(2)}, ..., a_{40}^{(2)}] \oplus C[b_1^{(2)}, b_2^{(2)}, ..., b_{40}^{(2)}] = K[c_1^{(2)}, c_2^{(2)}, ..., c_{40}^{(2)}]$  
iii. $P[a_1^{(3)}, a_2^{(3)}, ..., a_{40}^{(3)}] \oplus C[b_1^{(3)}, b_2^{(3)}, ..., b_{40}^{(3)}] = K[c_1^{(3)}, c_2^{(3)}, ..., c_{40}^{(3)}]$  
iv. $P[a_1^{(4)}, a_2^{(4)}, ..., a_{40}^{(4)}] \oplus C[b_1^{(4)}, b_2^{(4)}, ..., b_{40}^{(4)}] = K[c_1^{(4)}, c_2^{(4)}, ..., c_{40}^{(4)}]$ 

hold with probabilities $p_1 = .75$, $p_2 = .7$, $p_3 = .8$, $p_4 = .9$, respectively.

Suppose that on 10 plaintext/ciphertext pairs the LHS of i, ii, iii and iv “vote” that the RHS of the equations are 0 with tallies (2,8,2,8)

What is the probabilities that each of the most popular choices for the resulting constraints is correct? What is the probability that all 4 are correct? If all 4 are correct, and assuming $X$ takes 1 microsecond/encrypt, what is the time to break $X$ by exhaustive search (assuming a serial processor)? How about by applying the 4 constraints and searching for the remaining key bits (assuming a serial processor)?  

PS: Key search is a “trivially parallelizable” operation.
(E) In the lecture we noted that there was a linear attack that worked on 16 round DES with $2^{43}$ plaintext/ciphertext pairs where the basic constraint held with probability $p = \frac{1}{2} + \epsilon$ where $\epsilon = 1.19 \times 2^{-21}$ is the “bias”. Using this fact, estimate for what $p$, there are not enough corresponding plain/cipher texts to enable applying the Linear cryptanalysis to reduce the search keyspace.