Problems with traditional systems

- We assume that an attacker has at least some knowledge of the statistical characteristics of the plaintext.
- If these statistics survive in the ciphertext, the cryptanalysis may be able to greatly restrict the key space.
Twin goals of modern encryption

- **Confusion**: Make the statistical relationship between the ciphertext and the key value as complex as possible.
- **Defusion**: Dissipate the statistical structure of plaintext throughout the ciphertext.

Modern convention algorithms attempt to achieve this using substitution-permutation networks.

Production of pastry dough

- Shannon pointed out that the composition of non-commuting encryption methods works like a thorough pastry dough mixing.
- Iterating the product encryption increases the mix.*

*Unfortunately, all bets are off if the methods commute as is the case of a Caesar cipher and a simple transposition.
Modular transformation

- Consider the composition of a reflection with an affine distortion followed by a reduction to the basic format by cutting off and pasting back protruding corners.

\[
T:\begin{cases}
  x = y \\
  x + y = 1 & \text{if } x + y \geq 1 \\
  x + y = 0 & \text{if } 0 \leq x + y < 1
\end{cases}
\]

Mixing F.L. Bauer

- Applying this method to a picture of the cryptographer F.L. Bauer does seem to result in a total mix.
The resurrection of F.L. Bauer

- However, in the discrete spaces of cryptography, any iteration of a fixed transformation is periodic.
- Texture turns up in our mix of FLB after only 48 steps, a fourfold ghost appears in the 192nd step.

Block ciphers

- A **stream cipher** encrypts a digital data stream one bit or one byte at a time.
- A **block cipher** encrypts blocks of plaintext as a whole.
- The vast majority of **network-based conventional cryptographic applications** use block ciphers.
In early 70s, Horst Feistel developed a sequence of fixed transpositions and key-dependent, multipartite non-linear substitutions that produced a thorough amalgamation.

Feistel was successful enough to upset the NSA.

LUCIFER was not chosen as the national standard, DES was.

However, DES reflects the classic 64-bit Feistel block structure.*

*Unfortunately, restricted to 56 bit keys by the NSA.
**Simplified DES**

Key generation for S-DES

Key generation for S-DES

---

*Developed by E. Schaefer at Santa Clara University as a teaching tool.*
Initial and final permutations

The function $f_K$

- The most complex component of S-DES is the function $f_K$.
- It can be expressed as

$$f_K(L, R) = (L \oplus F(R, SK), R)$$

where $L, R$ are the left and rightmost four bits of input, $F$ is the inner gray box, and $SK$ is subkey.
The inner gray box

- The first operation is an expansion/permutation:
  \[ E/P = (4\ 1\ 2\ 3\ 2\ 3\ 4\ 1) \]
- Result is XORed with subkey, and fed into two S-boxes:

\[
\begin{align*}
S_0 &= \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 2 & 3 & 1 & 3 \end{bmatrix} & S_1 &= \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}
\end{align*}
\]

- The output of \( S_0 \) and \( S_1 \) is permuted once more:
  \[ P_4 = (2\ 4\ 3\ 1) \]

---

Pastry dough mixing*

*The left and right 4 bits are switched (SW) and we do it again with a new subkey.*
Analysis of S-DES

- With a 10-bit key, S-DES is vulnerable to a brute-force attack.
- Alternating linear maps with nonlinear maps resulting from the S-boxes results in a complex polynomial expressions for the ciphertext bits, making cryptanalysis difficult.*

*In other words, a brute-force approach may be easiest. That's the best we can hope for.

Relationship of S-DES to DES
DES exhibits a strong avalanche effect

- A small change in either the plaintext or the key produces a significant change in the ciphertext.
- The two plaintexts differ by one bit (all zeros and a one followed by 63 zeros.)
- The two keys also differ by just one bit.

### Electronic codecook mode*

*Good enough for secure transmission of single values such as encryption keys.*
Ciphertext block chaining mode

Time to panic

- Millions was spent on fast hardware implementation of DES and it was the standard for many years.
- However a 56 bit key isn’t very big.

<table>
<thead>
<tr>
<th>Key Size (bits)</th>
<th>Number of Alternative Keys</th>
<th>Time required at 1 encryption/s</th>
<th>Time required at 10^9 encryption/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>$2^{40} = 4.3 \times 10^{12}$</td>
<td>$2^{40} \mu s = 35.6$ minutes</td>
<td>$2.15$ milliseconds</td>
</tr>
<tr>
<td>56</td>
<td>$2^{56} = 7.2 \times 10^{16}$</td>
<td>$2^{56} \mu s = 1142$ years</td>
<td>$10.01$ hours</td>
</tr>
<tr>
<td>128</td>
<td>$2^{56} = 7.2 \times 10^{16}$</td>
<td>$2^{56} \mu s = 5.4 \times 10^9$ years</td>
<td>$5.6 \times 10^9$ years</td>
</tr>
<tr>
<td>26 characters (permutation)</td>
<td>$2^{60} = 4 \times 10^{18}$</td>
<td>$2^{60} \mu s = 6.4 \times 10^7$ years</td>
<td>$6.4 \times 10^7$ years</td>
</tr>
</tbody>
</table>
Double DES

- The answer is simple, we choose two keys $K_1, K_2$ and run DES twice to obtain
  \[ C = E_{K_2}[E_{K_1}[P]] \, . \]
- Decryption requires that the keys be applied in reverse order
  \[ P = E_{K_1}[E_{K_2}[C]] \, . \]
- This scheme apparently involves a key length of
  \[ 56 \times 2 = 112 \text{ bits} \, . \]

![Diagram of Double DES](image)

Meet-in-the-middle attack

![Table for Meet-in-the-middle attack](image)
Triple DES with two keys

- An obvious counter to the meet-in-the-middle attack is to use three stages of encryption with three different keys.
- As an alternative, Tuchman proposed a triple encryption using only two keys \( C = E_{K_1} [D_{K_2} [E_{K_1} P ]] \)

Block cipher algorithms

- While triple DES remained the defacto standard for many years, it isn’t the fast kid on the block.*

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Clock cycles per round</th>
<th># of rounds</th>
<th># of clock cycles per byte encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blowfish</td>
<td>9</td>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>RC5</td>
<td>12</td>
<td>16</td>
<td>23</td>
</tr>
<tr>
<td>DES</td>
<td>18</td>
<td>16</td>
<td>45</td>
</tr>
<tr>
<td>IDEA</td>
<td>50</td>
<td>8</td>
<td>50</td>
</tr>
<tr>
<td>Triple-DES</td>
<td>18</td>
<td>40</td>
<td>108</td>
</tr>
</tbody>
</table>

*And now has been replaced by another Feistel block cipher AES.