Section 4 Lecture 25 - DES Implementation

One of the most widely-used and popular block ciphers was the Data Encryption Standard, superseded by the Advanced Encryption Standard in the early part of this millennium. Here we will look at the history and basic ideas behind the Data Encryption Standard – some more detail is on the lecture slides.

Data Encryption Standard (DES)

The *Data Encryption Standard* (usually referred to as *DES*) is often cited as the cipher that motivated the interest in cryptography and propelled the ideas of cryptanalysis.

The cipher was first developed in the early 1970s, and was adopted as an official standard in 1976. The intention from the US security agencies was to adopt a secure, common system, to be used throughout the US. Work between the US National Security Agency (NSA) and telecommunications giant IBM led to the formal definition of the cipher and its eventual adoption worldwide. Being described as "secure" it naturally motivated a deeper interest in cryptography as researchers took on the challenge to break it.

The Data Encryption Standard is theoretically a 64-bit block cipher (so uses a key of length 64 bits, and each message is split into blocks of 64 bits). However, the final 8 bits of the key are used as *parity bits* to ensure the integrity of the message. Hence, effectively the key length is only 56 bits.

This is a relatively short key length and eventually led to it being cracked. Why was it so short? The official view is that it was deemed sufficient for all purposes at the time by both IBM and the NSA. There are widespread suggestions that in actual fact, the NSA wanted a shorter key length to be adopted as an international standard, as they felt they had the computing power to be able to break the 56-bit in advance of the rest of the world and so put themselves at an advantage if it was adopted worldwide. These suggestions remain unproved and are only conjectures.

We will give the basic idea behind its operation without going into too much detail. Remember that this is a 64-bit cipher, and so takes in a block of length 64 (so we split our message into blocks of 64 bits, padding the final block if necessary.

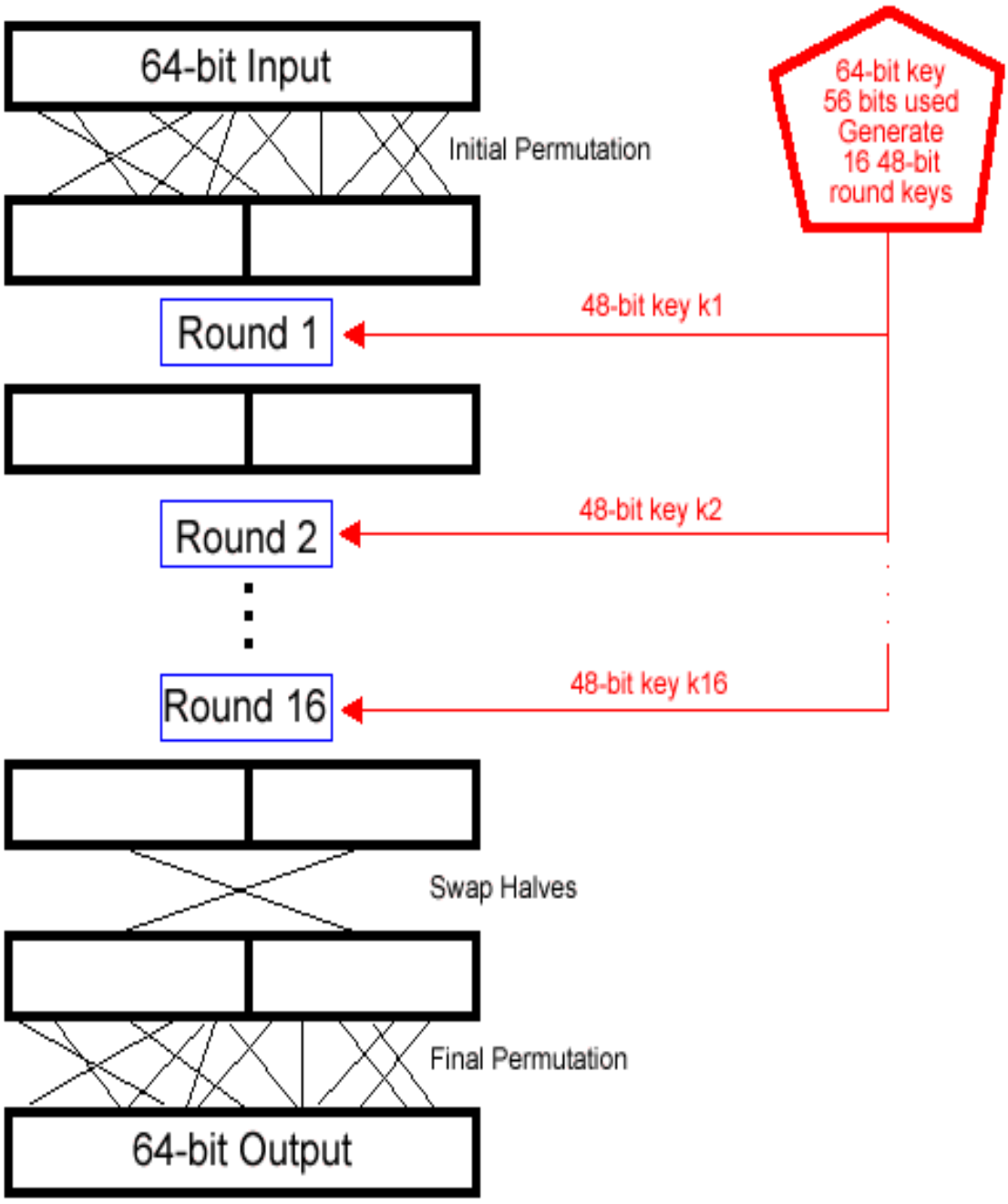
We start by permuting the bits under some random permutation (that is, we move the bits around) called the *initial permutation*. When finished, we apply the inverse of this, called the *final permutation*, to get everything back to normal. This isn't really an essential process but was done to ease the process of implementing the cipher on the hardware available.

In between, we apply a sequence of 16 identical *rounds* which act on the string of bits we currently have. Why 16? The real reason is that it's simply "enough" rounds to make the cipher secure. Only a few rounds are easy to crack, but having more than 16 doesn't really help to make the cipher any harder to crack.

After the original permutation, we split the message into two halves (so 32 bits each) and on each round, we act on only the first half and then swap the halves over.

The fundamental idea behind the action involves combining together the message bits and the key using the XOR operation. The advantage of using XOR is that if you were to apply it again (using the same keyword) then you get the original message back again. So decryption is easy – this is a feature of "symmetric" algorithms where the same key is used for encryption and decryption.

The overall operation of the Data Encryption Standard is summarised in the diagram below (courtesy of Wikipedia)



This diagram illustrates the fact the original message is split into two halves, and one half is operated on at each stage. In each round, the whole scheme follows the *Feistel* scheme in what is known as an "F" (for Feistel) box. Without giving the full details, at each stage (in the "F" box) we:

- Expand the 32-bit half-block to 48 bits (standard algorithms exist to do this, for example duplicate every alternate bit)

- Derive a 48-bit key from the main 64-bit key using some algorithm (there will be a different key at each round), and take the XOR of these two 48-bit strings

- Split the answer into 8 mini-blocks of 6 bits, and apply a "substitution" to each mini-block to convert each one into a block of 4 bits (using some sort of fixed encryption scheme, for example looking up in a table a conversion for each possible mini-block)

- This leaves us with a 32 bit string, which we can apply a fixed permutation to and then get our final coded string. Note this is 32 bits long, just as the original half-block.

If this sounds complicated, even to explain at a basic level, that's because it is! Remember, this cipher was used on a global scale for the most sensitive of data. But if you know the key, it's a practical cipher because decryption is easy. Of course, keeping the key secret is a more difficult task.

The most important aspect of the cipher is the substitution stage, where the mini-blocks of length 6 are converted into blocks of length 4. This part of the process is the fundamental aspect of what makes the cipher secure.

Since the US Government had described it as "secure" it was a natural challenge to try and crack it. Cryptography as a subject really grew from here, as researchers, hackers and mathematicians worked towards cracking it and trying to prove it wasn't quite as secure as claimed. Theoretical attacks were put forward, although not practically implementable. However, in 1998 a machine "Deep Crack" was built by the Electronic Frontier Foundation which was able to crack the DES in less than 2 days. It's an entirely brute-force algorithm, it just keeps trying all possible keys, but computing power had grown to the level that this was actually feasible. The machine cost around $250,000 to build – a pittance for large corporations and governments.

The fact is, that although 56 bits was big enough when the cipher was invented in the 1970s, computing power has grown to such an extent that it was now practically breakable and 56 bits is just too small. You all know how computing power has grown – remember there wasn't even an internet when you were born, now can you imagine life without it? When the cipher was invented, the cost and time to create a machine to try every possible key was unimaginable and so it was considered secure. By the 1990s, it wasn't just imaginable, it was really practical!