THE STRENGTH OF DES

- The strength of DES fall into two areas: key size and the nature of the algorithm.

The Use of 56-Bit Keys :

- With a key length of 56 bits, there are 2^{56} possible keys, which is $7.2*10^{16}$ approximately keys. Thus, on the face of it, a brute-force attack appears impractical.
- Assuming that, on average, half the key space has to be searched, a single machine performing one DES encryption per microsecond would take more than a thousand years to break the cipher.
- As far back as 1977, Diffie and Hellman postulated that the technology existed to build a parallel machine with 1 million encryption devices, each of which could perform one encryption per microsecond. This would bring the average search time down to about 10 hours. The authors estimated that the cost would be about $20 million in 1977 dollars.
- DES finally and definitively proved insecure in July 1998, when the Electronic Frontier Foundation (EFF) announced that it had broken a DES encryption using a special-purpose “DES cracker” machine that was built for less than $250,000.
- Hardware prices will continue to drop as speeds increase, making DES virtually worthless.
- There are a number of alternatives to DES, the most important of which are AES and triple DES.

The Nature of the DES Algorithm:

- Another concern is the possibility that cryptanalysis is possible by exploiting the characteristics of the DES algorithm.
- The focus of concern has been on the eight substitution tables, or S-boxes, that are used in each iteration. Because the design criteria for these boxes, and indeed for the entire algorithm, were not made public, there is a suspicion that the boxes were constructed in such a way that cryptanalysis is possible for an opponent who knows the weaknesses in the S-boxes.

- This assertion is tantalizing, and over the years a number of regularities and unexpected behaviors of the S-boxes have been discovered
- Despite this, no one has so far succeeded in discovering the supposed fatal weaknesses in the S-boxes

Timing Attacks:

- A timing attack is one in which information about the key or the plaintext is obtained by observing how long it takes a given implementation to perform decryptions on various ciphertexts.
- A timing attack exploits the fact that an encryption or decryption algorithm often takes slightly different amounts of time on different inputs.
- HEVI99 reports on an approach that yields the Hamming weight (number of bits equal to one) of the secret key. This is a long way from knowing the actual key, but it is an intriguing first step.
- The authors conclude that DES appears to be fairly resistant to a successful timing attack but suggest some avenues to explore.
- Although this is an interesting line of attack, it so far appears unlikely that this technique will ever be successful against DES or more powerful symmetric ciphers such as triple DES and AES