Miramontes Sarabia Luis Enrique
Criptografía 2020-1

Summary: Exhaustive Cryptanalysis of the NBS Data Encryption Standard

Cryptography has always been a valuable asset in our civilization, but has been shrouded in secrecy and mystery. The growing need of these systems requires a strong standard to keep up with the fast development of the field, unfortunately, the proposed standard (DES) is too weak for some applications and should be modified. The paper proposes a machine with a cost of 20 million able to break the DES standard for a cost of $5000 per solution in about 12 hours. Back in the day, this power was not available at everyone's house but intelligence agencies were able to finance one of these machines and in 10 years, the machine would decrease its cost to 200 thousand dollars.

The proposed standard transforms a plaintext of 64 bits into a cyphertext of 64 bits; the transformation uses a 56-bit invertible key. The attack will use a known plaintext to determine the key for use in later cyphertexts with an unknown key. The attack will use brute force using a million devices in parallel; the device has specific characteristics to break DES using minimal resource consumption.

One of the proposed arguments against the article says that increasing the key size to 128 bits or greater would increase the cost of the proposed machine but the key-related registers make up just 10% of the machine and increasing them would suppose a minimal increase of the machine's size. It would also challenge the storage capacity of magnetic cards that would need to double their storage size.

The machine's architecture consists of 64 racks for searching under the control of a mini-computer; each rack contains 128 circuits with 128 chips each. The total number of search units will be 2^{20}, slightly more than 1 million.

The chip uses CMOS/SOS for its low speed-power, being as low as 1pJ per gate and with delays of 5ns. The chip has a gate-density of 100 gates/mm^2, comparable with the Zilog Z80.

While looking at the algorithm there are two permutations that should be eliminated as they do not possess any cryptographic value and take 20% of the time needed for software implementation. Another fault in the standard is at the key scheduling algorithm, 8 bits are discarded to form a 56-bit key. The discarded bits are parity bits and is reasonable to discard them but if all 64 key bits were used giving the user a choice to forsake the parity check for an increased level of security the cost of a search would increase from $5000 to $1000000, increasing by a factor of 2^8. XORs are used to compute f(R,K) and for checking if the computed plaintext equals the known plaintext. If any of the 64-bit outputs is one, the chip tries the next key. If all the outputs are zero the key has been found.

As an afterword the authors believe a machine like this would be even more cheaper in the future considering how the prices were falling for components and how this were becoming faster and faster. It also proposes something that might resemble a dictionary of keys, that is a set of keys composed of eight ASCII characters from A to Z; as this ones are common in many applications and would be feasible to find them in less than one second at a really low cost. As a conclusion the usage of a 128-bit key is recommended to allow a margin of safety against shortcuts to exhaustive search.