Contents

1 Wide block cipher

A wide block cipher takes as input a fixed length K and an arbitrarily long message M and transforms it to C of the same length as M. It is a cipher were the bits of the cipher text depend on all the bits of the plain text. With stream ciphers every bit of the cipher text depends on one bit of the plain text.

Wide block ciphers are like a random permutation.

Wide block ciphers do not need a diversifier. There is no need for a diversifier because the C corresponding to similar M look completely different.

Block ciphers even provide data integrity. If Eve flips a bit in C a totally different M will come out that will probably look wrong. To ensure this you could add like 100 zeros to the end of your message and if it doesn't have that when you decrypt it you know someone flipped a bit. It does not protect against replay attacks as you can always try resend a valid message.

Sadly no one knows how to make a wide block cipher.

2 Block Cipher

The best thing we have is a block cipher (without wide). A block cipher is a cipher that takes fixed length key + fixed length message and then produces a fixed length C (b bits long) usually of the same size. For a fixed key K the mapping from P to C is invertible which means a block cipher performs a permutation, you write that as B_k and the inverse is B_K^{-1}.

If your message is b bits long then a block cipher is excellent for encrypting messages. However many messages are not b bits long. For messages that are less then b bits long have to do error-prone message manipulation and padding. When you have to do these things they almost fully evaporate the advantages of block ciphers.

You can still use block ciphers as a building block to build stream ciphers and mac functions. These ways of using block ciphers are called modes of uses.

The oldest block ciphers were Substitution-permutation networks (SPN). A cipher that was designed this way was DES. The successor of DES is AES

3 How do block ciphers work.

In a good block cipher each output bit depends on all input bits diffusion in a complicated way confusion. This is also the case the other way around. All the output of B on the cipher text depends on all the bits of the cipher text.

4 Statistical attacks on block ciphers

You can analyse a lot of plain text encrypted with the same key. Because these plaintext are encrypted with the same key and in the same way there are distingwishing properties that can be observed if a large number of results are obtained. This is usually done by looking at a where a is some intermidiate computation result in the encryption from P to C. The idea is that you can get a from$C$ by only guessing a small part of a key or even better a small part of the round key. If a has some statistical properties then the K_a you guessed is probably right. You can look at this like peeling of the last round of the encryption but it is nice because you only have to guess a small part of K or RK this small part is called K_a . There will be less possibilities for K_a because it has a shorter length and thus this is less guesses. Smart.

You want to have a distinguiser that has a high probablitiy of occuring. It things are random every bit can either be 0 or 1 so 1/2 chance for each. If your distinguiser says a certain bit is 1 if your k_a is correct and this chance is 70 percent then you might have the right k_a. If this is then the case for a large number of cipher text this is even more likely.

4.1 Differential cryptanalysis

With this one the distinguisher is a difference propagation with relatively high probability.

Given 2 random plaintext P and P' with difference DD_a the corresponding intermediate values a and a' with some probability. The difference between DD_p and DD_a is relatively high and can be considered independent from the cipher key K. This is called a high probability differencial and can be exploited like this:

Online Phase The adversary collects many pairs of plaintext-cipher text couples C and P and C' = P + DD_p

Offline Phase For all possible values of k_a the adversary computer the corresponding values of a and aand `checks if a +` a has the value DD_a for a fraction of $DP(DD_p, DD_a)$. This is going to be the case if you made the correct guess for k_a .

This works on DES with DP(DD_p, DD_a) = 2^{-47} where a is the input to the 14th round. What does DP mean? This attack is what we call academic because you need a lot of plaintext and ciphertext namely 1000 TB.

After this attack was published there was a concensious that block cipohers should not exhibit differentials with high probability.

4.2 Linear Crytanalysis

A linear cryptanalysis is where the distinguiser is a relatifely high correlation between the plaintext and an intermediate value. You find these values by applying masks to inputs and intermediate values and taking the results with the highest correlations. Then if you have found the pattern of bits in the plaintext and bits in the intermediate values you can search much faster because you only have to look the corresponsing bits. If the bits in a correlate to the bits in P then you probably have the right key. The hard part is finding the bits to focus on and this is done by looking at correlations between P and intermediate values.

Resistance against Linear and differential cryptanlysis is the basis of making a good cipher. In particular, the criterion is the absence of high-probability differentials and high input-output correlations, for the block cipher reduced by a few rounds. This now sounds obious but like Dijkstra said: Simplicity is a great virtue but it requires hard work to achieve it and education to appreciate it.