Breaking Block Ciphers using Repetition Codes

Benjamin Cutler

14th April 2003

Abstract

In January, 2003, Eric Filiol published a paper [1] describing an attack on block ciphers using repetition codes. If true this attack questions the security of all block ciphers. However another paper [2] was published by a group of individuals claiming that Filiol's attack is not valid. I describe the basis of the attack proposed by Filiol, and the results of the independent group that concluded why Filiol's attack was not valid.

Block Ciphers

- Block cipher E working on m-bit plaintext p and with a n-bit key k is a mapping $E : \mathbb{Z}_2^m \times \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^m$.
  - Each time a key k is chosen, this mapping reduces to a permutation over $\mathbb{Z}_2^m$
  $$c = E(p, k) = E_k(p)$$
  in order to decrypt c and get p back we need to have
  $$p = D_k(c) = E_k^{-1}(c)$$
  - This results in a total of 2^n possible permutations, which is a small subset of the total number of permutations: $(2^m)!$.

Block Ciphers

Notation: *let* $P_{\mathcal{E}}[\mathcal{I}]$ *denote the probability that a property* $\mathcal{I}$ *is satisfied over a set* $\mathcal{E}$.

- Suppose we have a key $K \in \mathcal{K}$, where $\mathcal{K} = \mathbb{Z}_2^n$, and a property $\mathcal{I}_K$ related to K such that $P_{\mathbb{Z}_2^m}[\mathcal{I}_K] \neq \frac{1}{2}$, then it is possible to recover the key K. We may attack a cipher if we can demonstrate that such a property $\mathcal{I}_{\mathcal{K}}$ exists for any $K \in \mathcal{K}$.

Repetition Codes

Binary Symmetric Channel (BSC) used to transmit messages over a binary alphabet. Takes a parameter p that describes the probability that a bit b_t will be effectively received.

- A n-repetition code is a $(n, 1)$ *linear code* with a minimum distance of n.
- Used for error detection and error correction purposes for a message sent over a BSC.
- For example a 3-repetition code an a message 01001 would be sent as 000 111 000 000 111. If 100 110 000 011 111 were received then the message would be decoded as 01011.

Block Cipher as a Binary Symmetric Channel

- Eric Filiol suggests the following [1]:

- Consider the plaintext space $\mathcal{P} = \mathbb{Z}_2^m$ and partition $\mathcal{P}_i$, $i \leq 2^k$, $k \in \mathbb{N}$. Suppose $P_{\mathcal{P}_i}[\mathcal{I}_{\mathcal{K}}] = p_i \neq \frac{1}{2}$ for some $\mathcal{P}_i$. We can compare the encryption process as a Binary Symmetric Channel because the key $K \in \mathcal{K}$ remains the same for all plaintext blocks.

- Treat encryption of N plaintext blocks $P \in \mathcal{P}_i$ as transmitting $\mathcal{I}_K$ using a N repetition code through a BSC.

- Attack the cipher using the Plaintext Dependent Repetition Code (PDRC) attack.

Resistance to PDRC Attack

- In order to be resistant to a plaintext-dependent repetition code attack, a block cipher must not have a property $\mathcal{I}$ such that $\mathcal{I}$ is biased in the output bits (i.e. $P_{\mathcal{C}_i}[\mathcal{I}] \neq \frac{1}{2}$, where $\mathcal{C}_i$ is a partition of the ciphertext space $\mathcal{C}$)

- Filiol's claim is that every block cipher has a property $\mathcal{I}$ such that $P_{\mathcal{C}_i}[\mathcal{I}] = \frac{1}{2}$, and hence no block cipher is immune to the PDRC attack.

Argument Against the PDRC Attack

- Nicolas T. Courtois, Robert T. Johnson, Pascal Junod, Thomas Pornin, and Michael Scott claim that Filiol was wrong [2].

- The biggest concern with the PDRC attack is AES, as AES is the new standard for encryption in government and industry.

- Courtois, et al., claim that none of Filiol's claims about biases in the output bits of AES hold true. They claim to have tested AES over many ciphertext blocks and haven't found any statistical information that supports the case for a bias in the output blocks of AES.

Conclusion

- Many tests have been done [2] by Courtois, et al., that demonstrate nothing unusual about the output bits of AES.

- As the new standard AES must remain under careful scrutiny to ensure that no unknown attacks against AES exist.

- However any newly published attack on any cipher (especially AES, as it is the new standard) must also be scrutinized to ensure that no false information regarding a cipher misleads people into believing that the cipher is insecure.

References

[1] Eric Filiol: *Plaintext-dependent Repetition Codes Cryptanalysis of Block Ciphers - the AES Case*, Published on eprint on 8th of January 2003. http://eprint.iacr.org/2003/003.

[2] Nicolas T. Courtois, et al.: *Did Filiol Break AES?*, Published on eprint on 4th of February 2003. http://eprint.iacr.org/2003/022.