Assignment 5

Abbas Khan , Mariia Rybalka , Linara Adilova

June 13, 2016

Task 5.1 (theoretical): Block Cipher Based MACs

Part (a)

- ECB gives encrypted with a shared secret blocks of a plain text. So basically this works as MAC for showing that the sender is the one, who knows shared secret and it can prove integrity because receiver can just decrypt the message and compare with received plain text. But by definition MAC has to be a short tag, and here it will be at best as long as the message itself. Also it is easily breakable because it saves the structure of the plaintext.

- CBC is usually used for generating MAC, by sending the last block. It will contain information about all the message and will be changed if the message is changed and also it will be encrypted by the shared secret, so it supports authenticity. The problem is with lots of known attacks, such as

- CTR is better than CBC in means of possibility to parallelise calculations, but like with ECB we need the whole encryption to support integrity, because here again all the blocks are different. It supports authenticity because of using shared secret for encryption.

Part (b)

[1]

References

[1] TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM) *https://tools.ietf.org/html/rfc5289*