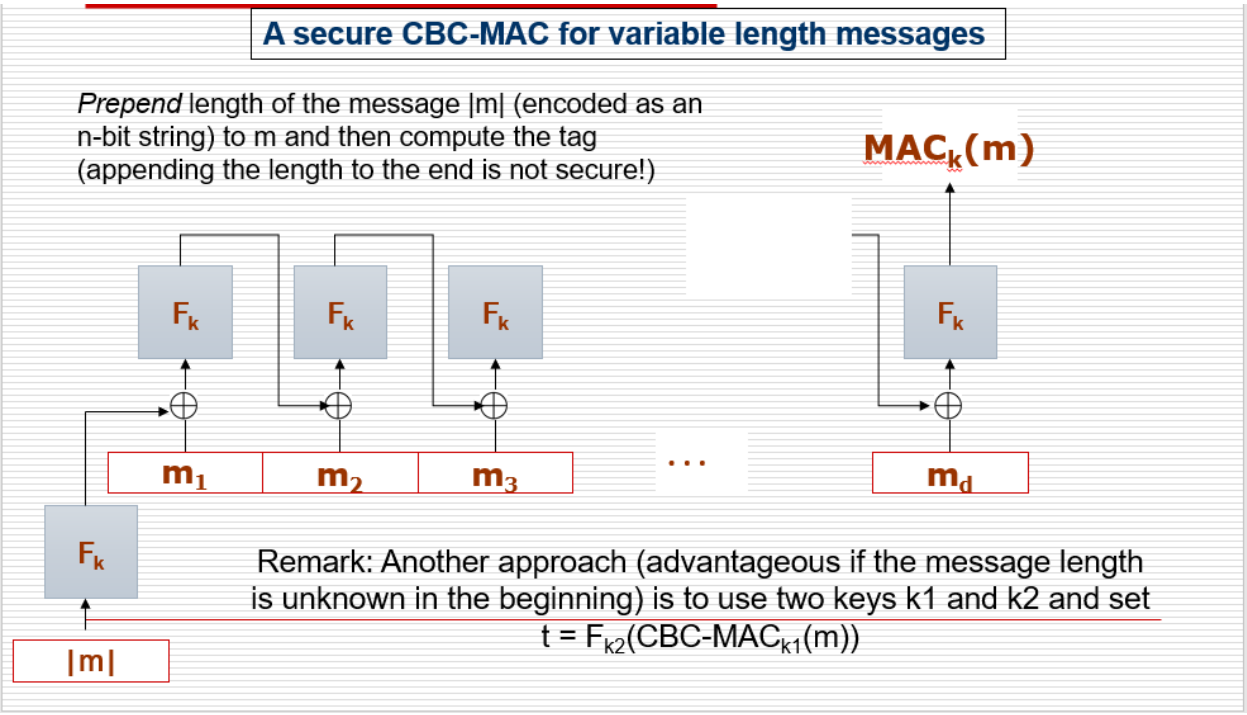
**2021201041**
**Nvss Maneesh Gupta**

**CCA Security – CBC MAC**

Even though the system is CPA secure it only gives confidentiality. There are some known CCA attacks where the adversary knows that what changes made in cipher text will reflect in plain text. So, CCA security is required to provide integrity.

To obtain integrity preserving the length (prefix attack), sequence number (permutation attack), random identifier (interleaving attack across messages) we use a naïve method to generate tag (MAC). But, the tag (MAC) obtained by the naïve method is much larger than the original plain text. Hence, we use CBC-MAC commonly called as CMAC.

**CBC MAC Construction**




Cipher Block Chaining is used to create the MAC with the message and initialization vector (IV). Here, $F_k$ is the PRF with the key k.

References

[1] J. K. a. Y. Lindell, Introduction to Modern Cryptography.

[2] B. Micali, "Hardcord bits," [Online]. Available: https://crypto.stanford.edu/pbc/notes/crypto/hardcore.html.

[3] Lecture Slides