Crypto X: Practical Message Authentication Codes

Cryptographic Hardware for Embedded Systems

ECE 3170

Fall 2025

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Reading Assignment

- Please read Chapter 18 part 14 of the course textbook by Schneier
- Also NOTE that these lecture notes contain updated information not contained in the course textbook by Schneier – you are still responsible for understanding this lecture!!!

Notation from Katz and Lindell

- $\{X\}$ is a set of elements of type X
- m is a message in plaintext
  - m is composed of smaller blocks m_i suitable for individual encryption steps
  - $m = \{m_i\}$
- c_i is ciphertext corresponding to message block m_i
- c is ciphertext corresponding to message m
- Enc_k is encryption with key k
  - $c \leftarrow Enc_k(m)$
- Dec_k is decryption with key k
  - $m \leftarrow Dec_k(c)$
- MAC_k is generation of a message authentication code t with key k
  - $t \leftarrow Mac_k(m)$ or, alternatively, $t \leftarrow Mac_k(c)$
- $<a,b>$ is a concatenation of a followed by b

Message Authentication

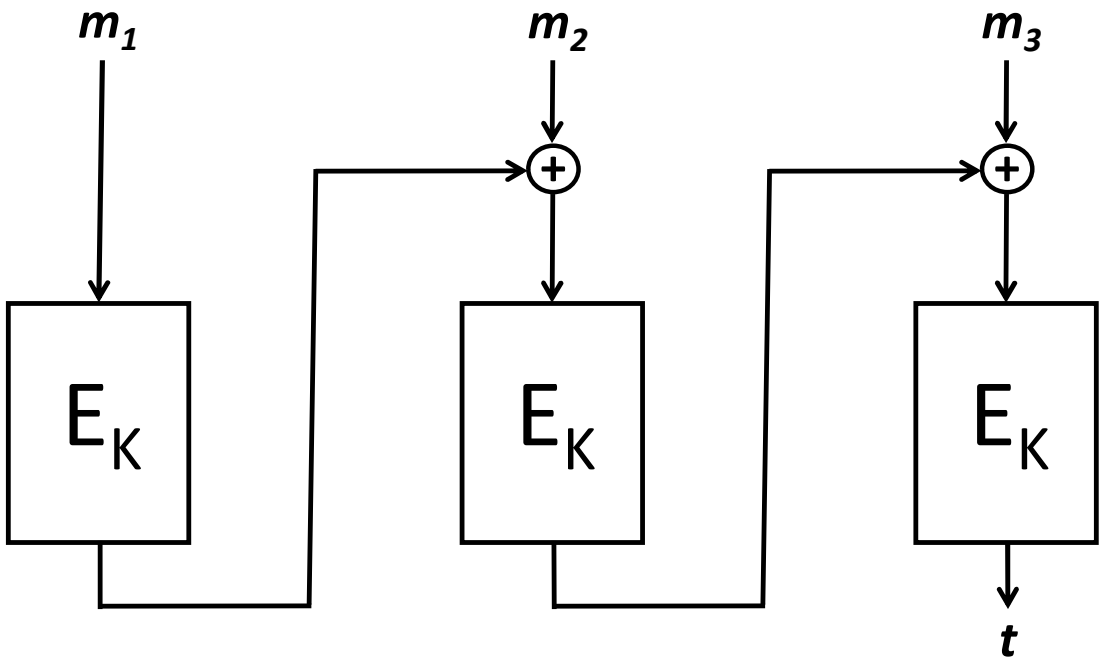
- Recall that authentication is the act of declaring something (e.g., a person, a message, or an item such as a car) to be authentic, where an identity is said to be authentic if the claimed identity truly corresponds to the thing (person, message, car, etc.)
- A message is authenticated if the identity of the sender is authenticated and the integrity of the message is verified
- We want to prevent *undetected* message tampering
- In this lecture we will describe a procedure we call a *Message Authentication Code* or MAC

Message Authentication Code (MAC)

- Traditionally MACs check message integrity
- Hence the name could perhaps more appropriately be called message integrity codes
- As covered in the previous lecture, state-of-the-art for entity authentication is to exchange nonces in initial messages
- A MAC would typically generate a small hash using a key

CBC-MAC

- Use results of previous block encryption
- Initialization Vector
  - optional
- MAC key should be different than encryption key, but the same encryption algorithm may be used



A Practical Variant

- In practice, key generation is considered to be expensive
- Add message length to the front, use same key as for message encryption