Cryptography 101: From Theory to Practice

Chapter 10 – Message Authentication

Rolf Oppliger

March 8, 2022

Terms of Use

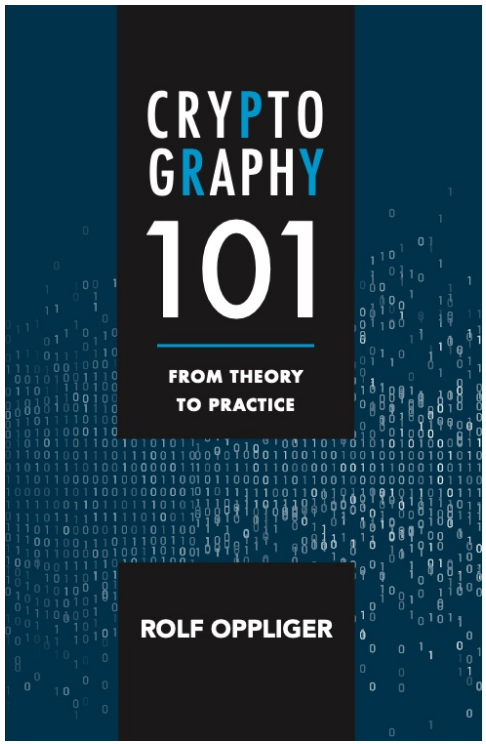
- This work is published with a CC BY-ND 4.0 license ()
  - CC = Creative Commons ()
  - BY = Attribution ()
  - ND = No Derivatives ()

whoami

rolf-oppliger.ch
rolf-oppliger.com

- Swiss National Cyber Security Centre NCSC (scientific employee)
- eSECURITY Technologies Rolf Oppliger (founder and owner)
- University of Zurich (adjunct professor)
- Artech House (author and series editor for information security and privacy)

Reference Book



ISBN 978-1-63081-846-3

`https://books.esecurity.ch/crypto101.html`

Challenge Me

Outline

10. Message Authentication

10. Message Authentication

10. Message Authentication

10.1 Introduction

- As its name suggests, an **authentication tag** is to authenticate a message
- This can be a digital signature or a **message authentication code (MAC)** — according to Definition 2.10
- Fundamental differences
  - A digital signature can provide nonrepudiation, whereas a MAC cannot
  - A digital signature can typically be verified by everybody, whereas a MAC can be verified only with the knowledge of the secret key

10. Message Authentication

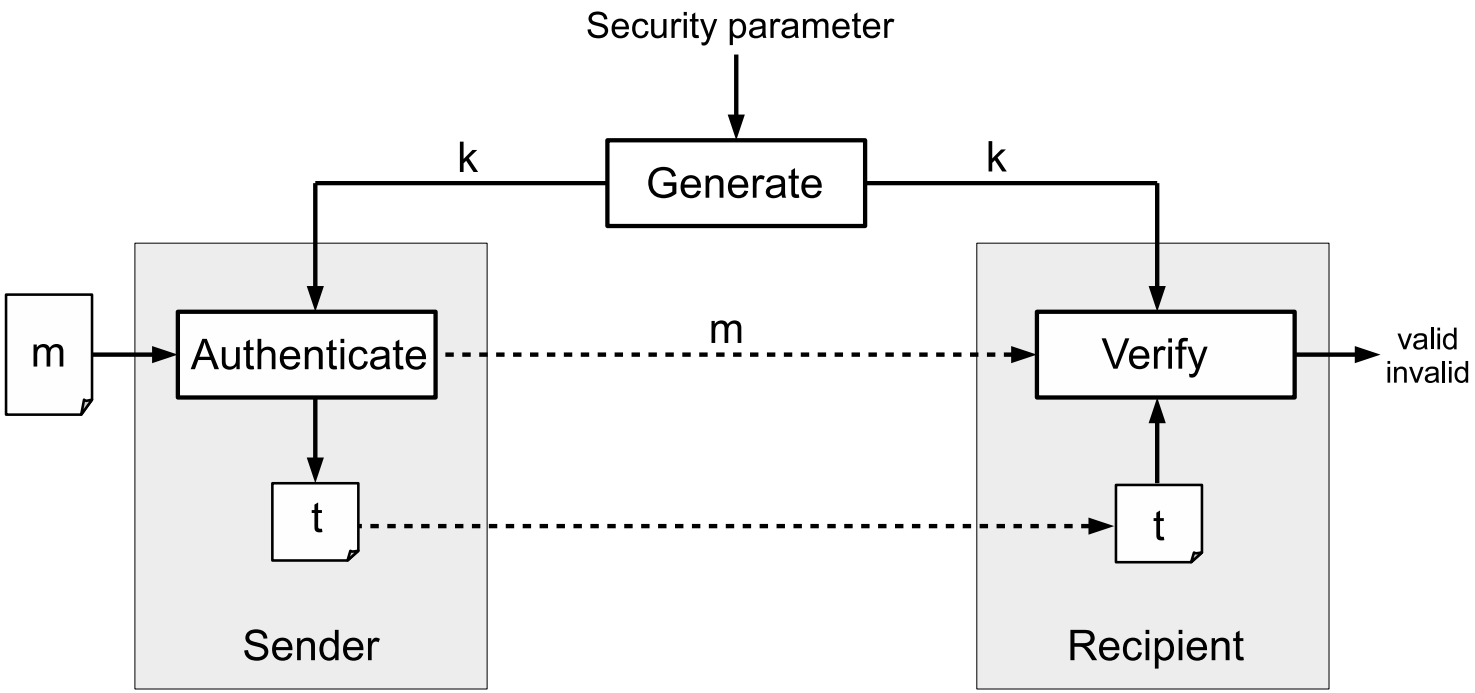
10.1 Introduction

- According to Definition 2.11, a **message authentication system** refers to a pair (A, V) of families of efficiently computable functions
  - $A : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ refers to a family $\{A_k : k \in \mathcal{K}\}$ of authentication functions $A_k : \mathcal{M} \to \mathcal{T}$
  - $V : \mathcal{K} \times \mathcal{M} \times \mathcal{T} \to \{valid, invalid\}$ refers to a family $\{V_k : k \in \mathcal{K}\}$ of verification functions $V_k : \mathcal{M} \times \mathcal{T} \to \{valid, invalid\}$

  For every message $m \in \mathcal{M}$ and key $k \in \mathcal{K}$, $V_k(m, t)$ must yield *valid* iff t is a valid authentication tag for m and k, i.e., $t = A_k(m)$ and hence $V_k(m, A_k(m))$ must yield *valid*

10. Message Authentication

10.1 Introduction



10. Message Authentication

10.1 Introduction

- To formally define the security of a message authentication system, one must define the attacks an adversary is able to mount and the task he or she must solve
- MAC-only attacks are pointless and irrelevant
- Relevant attacks
  - Known-message attacks
  - Chosen-message attacks (CMA)
- A CMA can be adaptive or nonadaptive

10. Message Authentication

10.1 Introduction

- Tasks (with decreasing severity)
  - Total break
  - Selective forgery
  - Existential forgery
- A MAC can always be guessed
- If the tag length is l_{tag}, then the respective success probability is $1/2^{l_{tag}}$
- This probability is negligible

10. Message Authentication

10.1 Introduction

- A MAC is (said to be) **unforgeable**, if a CMA-adversary can generate a valid message-tag pair with a success probability that is negligible
- Types of unforgeability (in some literature)
  - A MAC is **weakly unforgeable** under a CMA (WUF-CMA) if it is computationally infeasible for the adversary to find a message-tag pair for a "new" message
  - A MAC is **strongy unforgeable** under a CMA (SUF-CMA) if it is computationally infeasible for the adversary to find a new message-tag pair (i.e., the message may not be new)

10. Message Authentication

10.1 Introduction

- If a key is used to authenticate a single message, then information-theoretic securiy is possible
- This is similar to perfect secrecy in the realm of symmetric encryption (e.g., one-time pad)
- Such a MAC is called **one-time MAC (OTMAC)**
- The use of information-theoretically secure message authentication and OTMACs is prohibitively expensive
- Computationally secure message authentication and MACs (that are SUF-CMA) are used instead

10. Message Authentication

10.2 Information-Theoretically Secure Message Authentication

- The construction of an information-theoretically secure message authentication system in not difficult
- Many constructions are based on polynomial evaluation
- Example (due to Dan Boneh)
  - Let p be a prime that is slightly larger than the maximum value of a message block
  - If the block length is 128 bits, then a possible value is $p = 2^{128} + 51$
  - The key k consists of two parts, k_1 and k_2, that are both randomly chosen integers between 1 and $p - 1$, i.e., $k_1, k_2 \in_R [1, p)$

10. Message Authentication

10.2 Information-Theoretically Secure Message Authentication

- Example (continued)
  - The message m is cut into $l = \lceil |m|/128 \rceil$ 128-bit blocks $m[1], m[2], \ldots, m[l]$ that represent the coefficients of a polynomial $P_m(x)$ of degree l:

    $$P_m(x) = m[l]x^l + m[l-1]x^{l-1} + m[l-2]x^{l-2} + \ldots + m[2]x^2 + m[1]x$$

  - An OTMAC can then be defined as the modulo p sum of P_m evaluated at point k_1, i.e., $P_m(k_1)$, and k_2:

    $$OTMAC_k(m) = (P_m(k_1) + k_2) \bmod p$$

10. Message Authentication

10.2 Information-Theoretically Secure Message Authentication

- This construction is efficient and yields an information-theoretically secure OTMAC
- But it can be used to authenticate a single message
- If the same key is used to authenticate two or more messages, then the message authentication system gets totally insecure
- This means that an adversary is then able to construct MACs for arbitrary messages of his or her choice

10. Message Authentication

10.2 Information-Theoretically Secure Message Authentication

- There is a well-known construction to use the same key in a one-time message authentication system for multiple messages (with the same key)
- This construction is known as **Carter-Wegman MAC**
- The idea is to disguise (or encrypt) an OTMAC with a distinct random value (see below)
- Carter-Wegman MACs are "only" computationally secure but play an increasingly important role in the field

10. Message Authentication

10.3 Computationally Secure Message Authentication

- In general, there are three types of computationally secure message authentication systems
  - Systems that use a symmetric encryption system
  - Systems that use a keyed hash function
  - Systems that use Carter-Wegman MACs
- The first two types are further addressed in the multipart standard ISO/IEC 9797
- They can be combined in a specific way (e.g., $E_k(h(m))$)

10. Message Authentication

10.3 Computationally Secure Message Authentication

- Message authentication systems that use a symmetric encryption system (cipher)
  - CBC-MAC
  - CMAC
  - Parallelizable MAC (PMAC)
  - ...
- CBC-MAC and CMAC are conceptually similar, standardized, and widely used in the field

10. Message Authentication

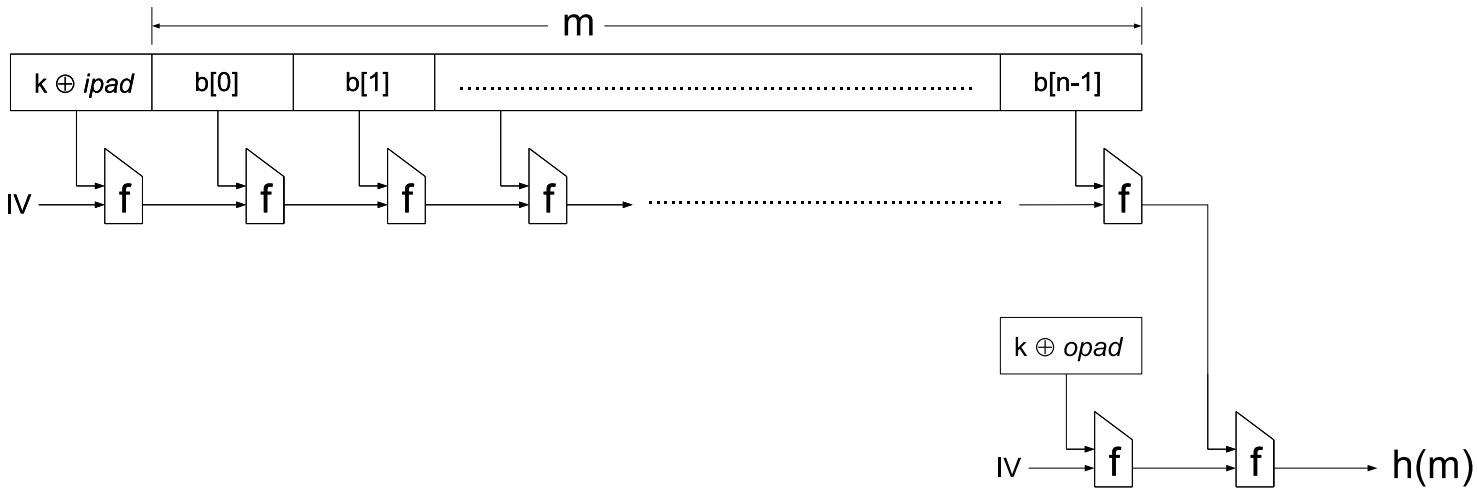
10.3 Computationally Secure Message Authentication

- Message authentication systems that use a keyed hash function h
  - Secret prefix method: $MAC_k(m) = h(k \parallel m)$
  - Secret suffix method: $MAC_k(m) = h(m \parallel k)$
  - Envelope method: $MAC_{k_1,k_2}(m) = h(k_1 \parallel m \parallel k_2)$
  - Nested MAC (NMAC)
  - Hashed MAC (HMAC)
  - KECCAK MAC (KMAC)
- The HMAC construction is most widely used in the field (e.g., together with SHA-1 or SHA-256)

10. Message Authentication

10.3 Computationally Secure Message Authentication

$$HMAC_k(m) = h(k \oplus opad \parallel h(k \oplus ipad \parallel m))$$



10. Message Authentication

10.3 Computationally Secure Message Authentication

- Message authentication systems that use Carter-Wegman MACs
  - The idea is to disguise (or encrypt) an OTMAC with a distinct random value r (nonce) using a PRF F
  - In addition to r, the construction usually requires two keys, i.e, k_1 and k_2:

$$CWMAC_{k_1,k_2}(m) = f_{k_1}(r) \oplus OTMAC_{k_2}(m)$$

  - There are different possibilities to instantiate this idea (or construction)

10. Message Authentication

10.3 Computationally Secure Message Authentication

- Examples
  - A block cipher in GCM authentication-only mode yields a Galois message authentication code (GMAC)
  - Poly1305-AES combines an OTMAC based on polynomial evaluation with AES as PRF:

$$\text{Poly1305-AES}_{k_1,k_2}(r,m) = (\text{AES}_{k_1}(r) + P_m(k_2)) \bmod 2^{128}$$

  - A universal MAC (UMAC) combines a OTMAC based on universal hashing with a PRF:

$$UMAC_{k_1,k_2}(m) = f_{k_1}(r) \oplus h_{k_2}(m)$$

10. Message Authentication

10.4 Final Remarks

- There are many possibilities to authenticate messages and to compute and verify respective MACs
- The HMAC construction is still predominant and most widely used in the field
- It is used, for example, in almost all Internet security protocols, including IPsec, SSL/TLS, and many more

10. Message Authentication

10.4 Final Remarks

- The HMAC construction usually employs an iterated hash function (e.g., SHA-1, SHA-256, . . .)
- This means that it operates sequentially
- There are security (e.g., Lucky 13) and performance issues, especially in high-speed networks
- There are alternative MAC constructions that can either be parallelized (e.g., PMAC) or otherwise operate more efficiently (e.g., Carter-Wegman MACs)

Questions and Answers

Thank you for your attention