Auto-Evaluation Questions
(Secure Hash Functions and MACs)

1. Define a secure hash function in terms of their properties.

2. What is different between a secure hash function and a secure hash based message authentication code?

3. In a secure hash function, what is the difference between weak collision resistance (or second pre-image resistance) and strong collision resistance?

4. Compare SHA-1, SHA-2-224, SHA-2-256, SHA-2-512 and whirlpool in terms of secure hash values produced and maximum input data or message size.

5. If a secure hash function produces an hash value of 384 bits, and considering that no cryptanalysis vulnerabilities exist, what is the probability to find a collision breaking the strong collision resistance assumptions?

6. Try to identify the security arguments and the practical advantages of using an HMAC construction for a Hash-based message authentication code protecting message authentication and message integrity

7. What is a CMAC and what are the security properties provided by CMAC functions?

8. What are the advantages of using HMACs comparing with CMACs? Do you believe the identified advantages are always valid, independently of the cryptographic algorithms used for the HMAC and CMAC constructions?

9. What are the advantages of using CMACs comparing with HMACs? Do you believe the identified advantages are always valid, independently of the cryptographic algorithms used for the HMAC and CMAC constructions?

10. Do you believe that the strong collision resistance of a secure hash function, as theoretically defined, is possible in practice? Discuss the answer with a valid argumentation.

11. State the value of the padding field in SHA-512 when the input message has a length of: a) 4987 bits; b) 4199 bits; c) 1227 bits

12. State the value of the length field in SHA-512 when the input message has a length of: a) 3967 bits; b) 3968 bits; c) 3969 bits

13. It is possible to use a HASH function to construct a symmetric block-cipher with a structure similar to DES. Try to propose such a symmetric encryption. Remember that a secure hash function in its base is “one way”, but a symmetric block cipher must be reversible, using the proper cryptographic key. Do you have a solution for this ?

14. A user Ui will use a password for authentication on the server S. S has a database with entries in the following form, and we consider that there are no intrusion attacks against S.

    usernameU1: $H_{SHA\text{-}2\text{-}256}$ (pwdU1): K1

    usernameU2: $H_{SHA\text{-}2\text{-}256}$ (pwdU2): K2

    …

    usernameUi: $H_{SHA\text{-}2\text{-}256}$ (pwdUi); Ki

    usernameUn: $H_{SHA\text{-}2\text{-}256}$ (pwdUn): Kn

    For authentication, A sends:
    E_{Ki} (usernameUi || pwd)|| MAC_{Ki} (usernameUi))

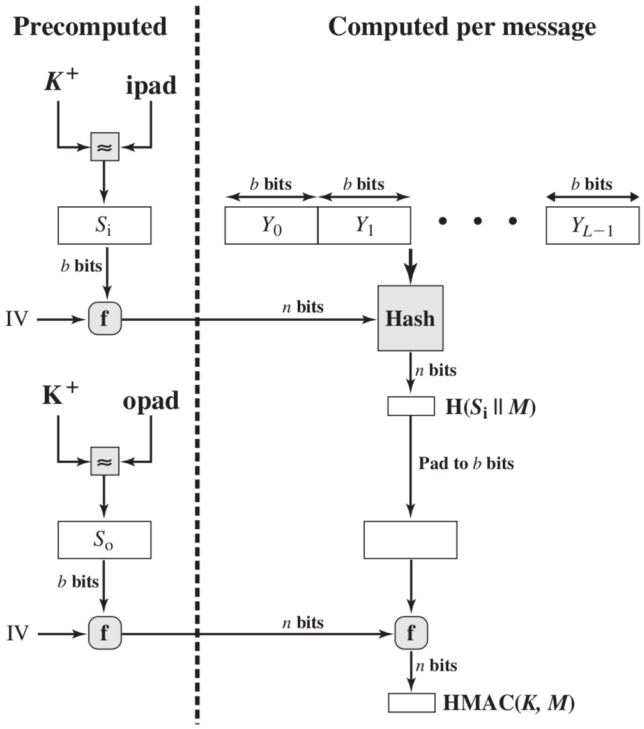
    Do you believe the solution works and can provide a secure authentication of users by the server S ?

15. In this problem, we will compare the security services provided by message authentication codes (CMAC). We assume that Oscar is able to observe all messages send from Alice to Bob and vice versa. Oscar has no knowledge of any keys that can be shared between Alice and Bob. State whether and how CMAC protect against each attack in the following questions. The value auth(x) is computed with MAC algorithm, respectively.

    a) (Message integrity) Alice sends a message x = "Transfer $1000 to Mark" in the clear and also sends auth(x) to Bob. Oscar intercepts the message and replaces "Mark" with "Oscar". Will Bob detect this?
    b) (Replay) Alice sends a message x = "Transfer $1000 to Oscar" in the clear and also sends auth(x) to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?
    c) (Sender Authentication with cheating third party) Oscar claims that he sent some message x with a valid auth(x) to Bob, but Alice claims the same. Can Bob clear the question in either case?
    d) (Authentication with Bob cheating) Bob claims that he received a message x with a valid signature auth(x) from Alice (e.g., "Transfer $1000 from Alice to Bob") but Alice claims she has never sent it. Can Alice clear this question in either case?
    e) There are differences in your answers in a) to d) if auth(x) is computed with a HMAC and not with a CMAC construction?

16. The following figure shows an alternative HMAC implementation.

    a) Describe the operation of this implementation.
    b) What potential benefit do you recognize in this implementation compared with the HMAC construction based in the RFC 2408 standard?


Precomputed
Computed per message
K+
ipad
≈
Si
b bits
IV
f
b bits
b bits
b bits
Y0
Y1
YL−1
n bits
Hash
n bits
H(Si || M)
Pad to b bits
K+
opad
≈
So
b bits
IV
f
n bits
f
n bits
HMAC(K, M)