# Review Questions

1. What is the difference between authentication and signature?

2. Does encryption alone provide authentication? Explain why or why not.

3. What is the advantage of using message authentication codes over encrypting hash code?

4. What is the weakness in CBC-MAC? How is it solved in CMAC?

# Problems

For each of the following usages of hash or cryptographic function:

|  |  |  |  |
| --- | --- | --- | --- |
| a. | X🡪 Y: E(K, [M || H(M)]) | b. | X 🡪 Y: M || H(M||S) |
| c. | X 🡪 Y: M || E(PRx, H(M)) | d. | X 🡪 Y: E(PUy, [M || C(K, M)]) |

Where X, Y are the two communicating parties. M = message. H = hash function. C = MAC function. S is a secret value known only to X and Y. K = secret key.

1. Draw a diagram showing the operation and the reverse operation.

2. Explain what security services provided (confidentiality, authentication, signature).

3. Propose an alternative method, if applicable, to provide the same security services.

4. Formulate the following problems in terms of security requirements, then suggest the correct procedure to solve each problem:

a. Two people (Ahmed and Badr) would like to communicate with each other. They don’t have any pre-shared secret information. They don’t want other people to spy on their communication.

b. A bank wants to protect its clients when using online banking. Clients tend to use easy passwords. Someone may steal the password and be able to access the client’s account.

c. A bank wants to allow clients to request services on their accounts using email. The bank wants to have a proof that the actual client is the one who sends the email so that they don’t deny it in the future.