Information Integrity and Authentication

IMPORTANT NOTES:
Study lecture materials at least 1 hour and prepare Q1-6 prior to the tutorial session. Prepared questions will be discussed in the tutorial session.

1. Briefly describe three main use of digital signature.

2. Describe the stages of generating and verifying the RSA digital signature for long documents.

3. Discuss features of a good one-way hash function.

4. Discuss digital signature requirements.

5. What is Message authentication?

6. What are three requirements for MAC?

7. For n=77, e=13 and d=37 what is the value of a RSA digital signature of message M=15? ($15^5 \bmod 77 = 1$). Assume the basic (textbook) RSA signature where no hash function is used.

8. For n=77 e=17 the value of a RSA digital signature for message M=12 is 45. Show the verification process ($9^{15} \bmod 77 = 1$, $5^{15} \bmod 77 = 34$). Assume the basic (textbook) RSA signature where no hash function is used.

9. List two disputes that can arise in the context of using Message Authentication Codes (MACs).

10. Suppose $H(m)$ is a collision resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all messages x, x' with $x \neq x'$, we have $H(x) \neq H(x')$? Explain your answer.

Optional Questions for Further Exploration

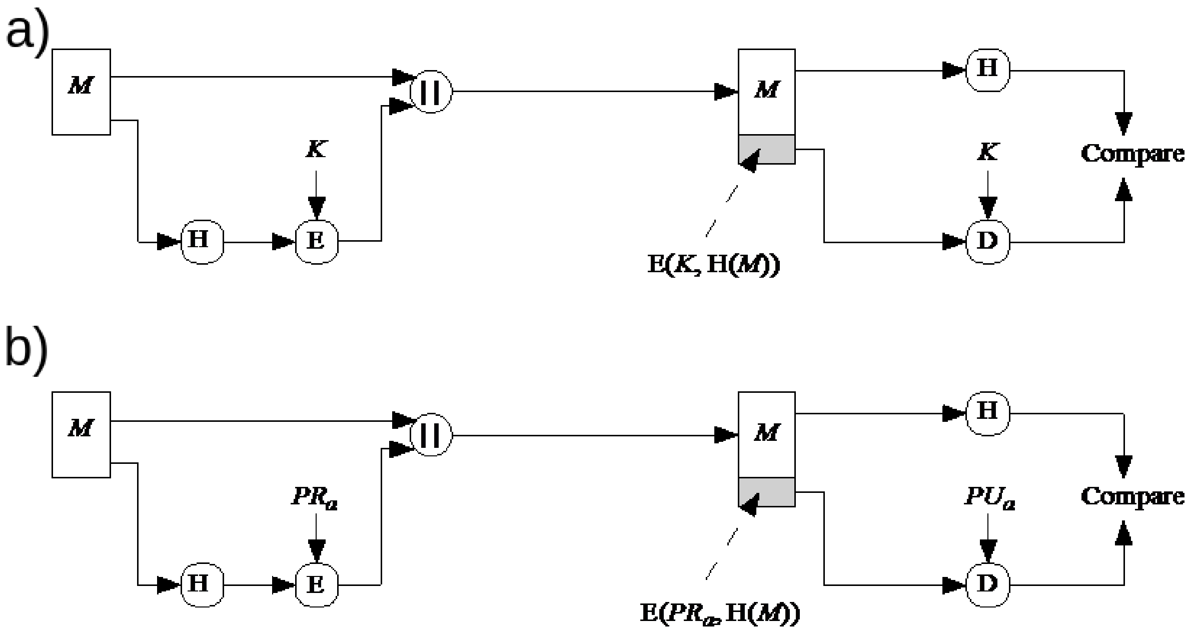
1. What is the difference between a message authentication code and a one-way hash?

2. With regards to a n-bit output hash function H with $n \geq 32$:

   (a) How long does it take on average for a brute force attack to find a message M such that $H(M)$ has 32 **zero** leading (leftmost) bits? Note that in this case, the $n - 32$ trailing (rightmost) bits of $H(M)$ can be arbitrary. Assume that the output of the hash is evenly distributed and each input is independent.

   (b) How long does it take on average for a brute force attack to find two messages M_1 and M_2 such that $H(M_1)$ and $H(M_2)$ collide on the 32 leading bits? Note that in this case the string of 32 leading bits of $H(M_1)$ must equal the string of 32 leading bits of $H(M_2)$ though the value of that 32 bit string can be arbitrary, while the trailing $n - 32$ bits of $H(M_1)$ and $H(M_2)$ can be arbitrary and unequal bit strings.

3. The following figure illustrates two methods in which a hash code can be used to provide message authentication. Explain both methods.


a)
M
K
H
E
||
M
H
K
Compare
D
E(K, H(M))
b)
M
PR_a
H
E
||
M
H
PU_a
Compare
D
E(PR_a, H(M))