FIT2093: Tutorial 8

Digital Signature & Integrity Management

Review

1. Briefly describe two main use of digital signature.
2. Describe the stages of generating and verifying digital signature for long documents.
3. Discuss features of a good one-way hash function.
4. Name desirable features of digital signature.
5. Discuss digital signature requirements.
6. What is Message authentication?

7. What are the three requirements for MAC?

8. Why use a MAC rather than a message encryption for authentication functions? Give two reasons.

9. List 3 possible methods that can be used for message authentication.

Problems

1. A hash function is defined as the sum of the value of each character in the message modulus 26 (Table 1). For instance the hash value of ABC is 0 + 1 + 2 = 3 mod 26 = 3. If n = 55 and e = 7 and d = 23 what is the value of digital signature for message "DOG" and message "TEST"? (23^4 mod 55 = 1 and 23^2 mod 55 = 34 and 8^{20} mod 55 = 1)

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

Table 1

2. For the hash function given in previous problem discuss the five features of a good hash function.

3. For n=77, e=13 and d=37 what is the value of digital signature of message M=15? (15^5 mod 77=1)
4. For n=77 e=17 the value of digital signature for message M=12 is 45. Show the verification process (9^{15} mod 77 =1, 5^{15} mod 77 =34).
5. What protective measure can be used to counter source repudiation? Can it be used to counter destination repudiation?
6. List two disputes that can arise in the context of message authentication.

7. 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 ≠ x', we have H(x) ≠ H(x')? Explain your answer.

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

9. The data authentication algorithm, described in Section 11.3, can be defined as using the cipher block chaining (CBC) mode of operation of DES with an initialization vector of zero (Figure 1). Show that the same result can be produced using the cipher feedback mode.

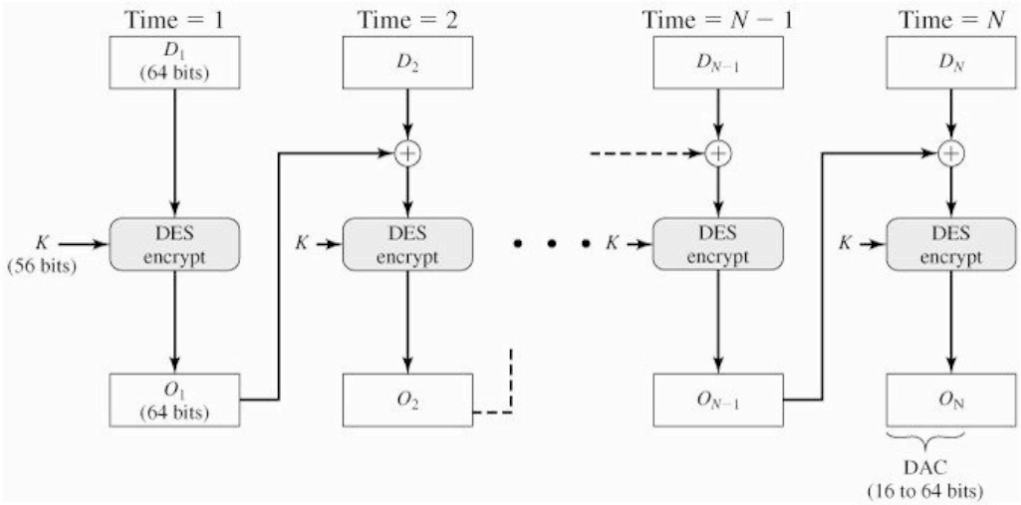

Figure 1 Data Authentication Algorithm (FIPS PUB 113)

10. Figure 2 illustrates six methods in which a hash code can be used to provide message authentication. Explain each of the six methods.

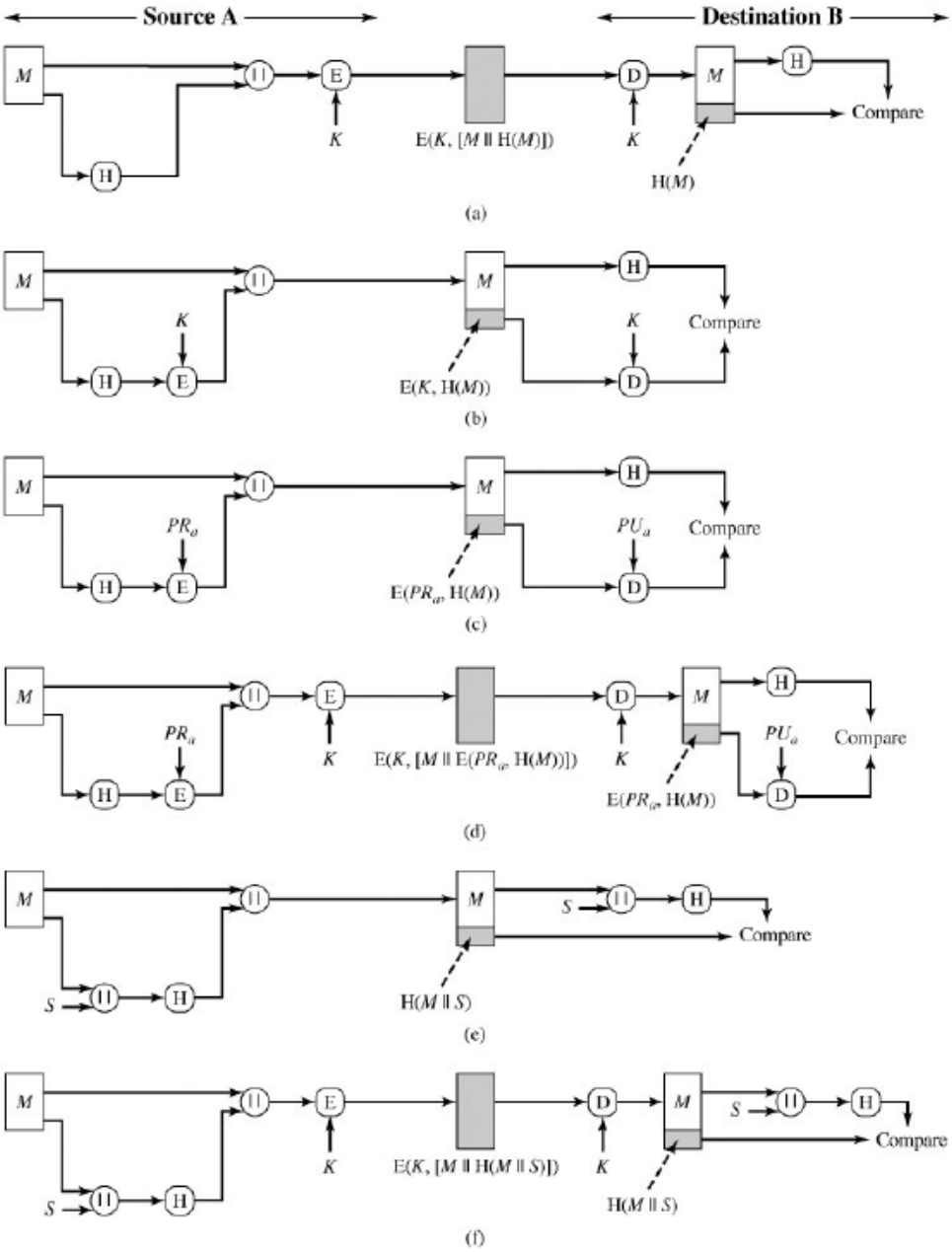

Figure 2 Basic Uses of Hash Function