FIT2093: Sample Tutorial 8 Solutions

Digital Signature & Integrity Management

Review

1. Briefly describe two main use of digital signature.

Digital signature is used for non-repudiation as it can prove the authenticity of the signer

Another use of digital signature is to ensure the integrity of the messages if it contains information about data that cannot be forged

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

Signature Generation

   a. Generate the message digest of the document using a (secure) one-way hash function
   b. Encrypt the message digest with private key of the signer
   c. Attach the signature to the message

Signature Verification

   a. Generate the message digest for received document using the same (secure) one-way hash function
   b. Decrypt the attached signature using public key of the signer
   c. Compare the decrypted digest with generated one if a match verification is successful

3. Discuss features of a good one-way hash function.
   a. Can be applied to any size of data: files and messages with arbitrary sizes can be signed
   b. Produces a fixed-length output: overhead of signature for transmission or storage is low and the verification process is easier
   c. Fast and efficient algorithm: signature generation and verification should be fast and efficient (low overhead in terms of processing time)
   d. One-way feature: infeasible to get back message from the hash value
   e. Hard to find collisions: it should be infeasible to find two inputs that will be hashed into the same value

4. Name desirable features of digital signature.
   a. Non-forgeable
   b. Undeniable by the signatory
   c. Universally verifiable
   d. Different for different documents

e. Easily implementable

5. Discuss digital signature requirements.
   - Must be a bit pattern based on the message being signed
   - Must use some information unique to the sender (prevent forgery and denial)
   - Relatively easy to produce
   - Relatively easy to recognize and verify
   - Computationally infeasible to forge by either constructing a new document with the same digital signature or forge a signature for a document
   - Must be practical to retain a copy of the digital signature

6. What is Message authentication?

   Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent by (i.e., contain no modification, insertion, deletion, or replay) and that the purported identity of the sender is valid.

7. What are three requirements for MAC?

   a. Knowing a message and MAC, is infeasible to find another message with same MAC
   b. MACs should be uniformly distributed across the messages
   c. MACs should depend equally on all bits of the message

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

   - Sometimes only authentication is needed
   - Sometimes need authentication to persist longer than the encryption (eg. archival use)

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

   - message encryption
   - message authentication code (MAC)
   - hash function

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

H(DOG) = 3+14+6 mod 26 = 23
Signature = H(m)^d mod n = 23^{23} mod 55 = (23^4 mod 55)^5 * (23^3 mod 55) = 23*34 mod 55 = 782 mod 55 = 12

H(TEST) = 19+4+18+19 mod 26 = 60 mod 26 = 8
Signature = H(m)^d mod n = 8^{23} mod 55 = (8^{20} mod 55) * (8^3 mod 55) = 8 * 64 mod 55 = 8*9 mod 55 = 72 mod 55 = 17

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

Input size: can be applied to any input size
Fixed-length output: will generate a number in interval [0-25]
Fast algorithm: the algorithm only uses addition operation and a modulus
One-way: It is infeasible to get back the exact same message from the value of the hash
Hard to find collisions: it is easy to find collisions for messages words can be replaced with other words with the same value, words can be added or remove as long as the final value would be the same. (Anagrams can be used such as DEAR and READ or MILES and SMILE, LEADER and DEALER)

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)

Signature = M^d mod n = 15^{37} mod 77 = (15^5 mod 77)^7 * (15*15 mod 77) = 225 mod 77 = 71

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).

$(Sig)^e$ mod n = M
45^{17} mod 77 = [(5*9)^{15} mod 77]*[(5*9)^2 mod 77] = (5^{15} mod 77)*(9^{15} mod 77)*(81 mod 77)*(25 mod 77) = (34 * 1 * 4 * 25 mod 77) = 34 * 100 mod 77 = 34 * 23 mod 77 = 782 mod 77 = 12 = M (Signature is verified)

5. What protective measure can be used to counter source repudiation? Can it be used to counter destination repudiation?

Digital signature
The signatory of the message uses his private key to sign the message. Since the private key is only known by the signatory he cannot deny signing the message.

If the destination signs a receipt or acknowledgement with his own private key and send it back to the sender yes otherwise the receiver can deny that he received the signed document.

6. List two disputes that can arise in the context of message authentication.

   Suppose that John sends an authenticated message to Mary. The following disputes that could arise: 1. Mary may forge a different message and claim that it came from John. Mary would simply have to create a message and append an authentication code using the key that John and Mary share. 2. John can deny sending the message. Because it is possible for Mary to forge a message, there is no way to prove that John did in fact send the message.

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 $x \neq x'$, we have $H(x) \neq H(x')$? Explain your answer.

   The statement is false. Such a function cannot be one-to-one because the number of inputs to the function is of arbitrary, but the number of unique outputs is 2^n. Thus, there are multiple inputs that map into the same output.

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

   A hash function, by itself, does not provide message authentication. A secret key must be used in some fashion with the hash function to produce authentication. A MAC, by definition, uses a secret key to calculate a code used for authentication.

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.

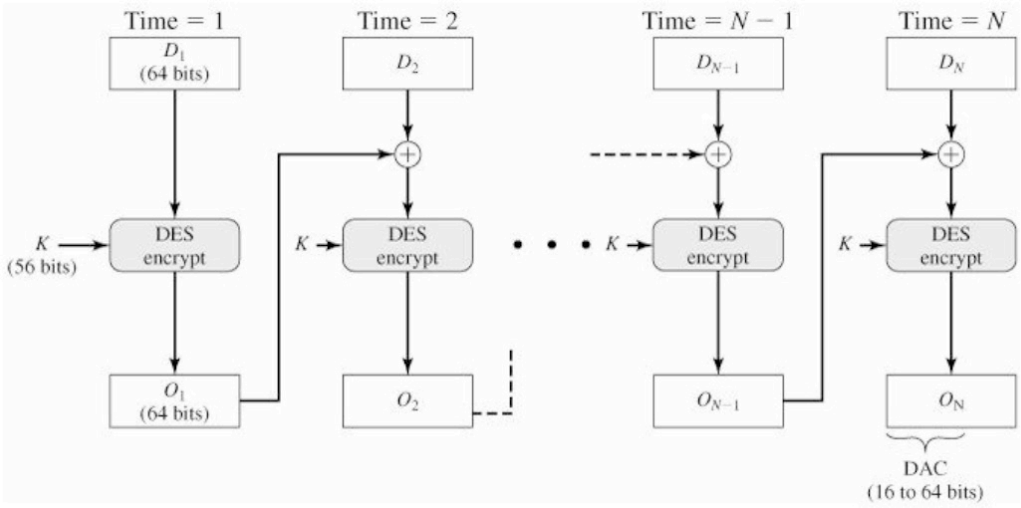

Figure 1 Data Authentication Algorithm (FIPS PUB 113)

The CBC mode with an IV of 0 and plaintext blocks D1, D2, . . ., Dn and 64-bit CFB mode with IV = D1 and plaintext blocks D2, D3, . . ., Dn yield the same result

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

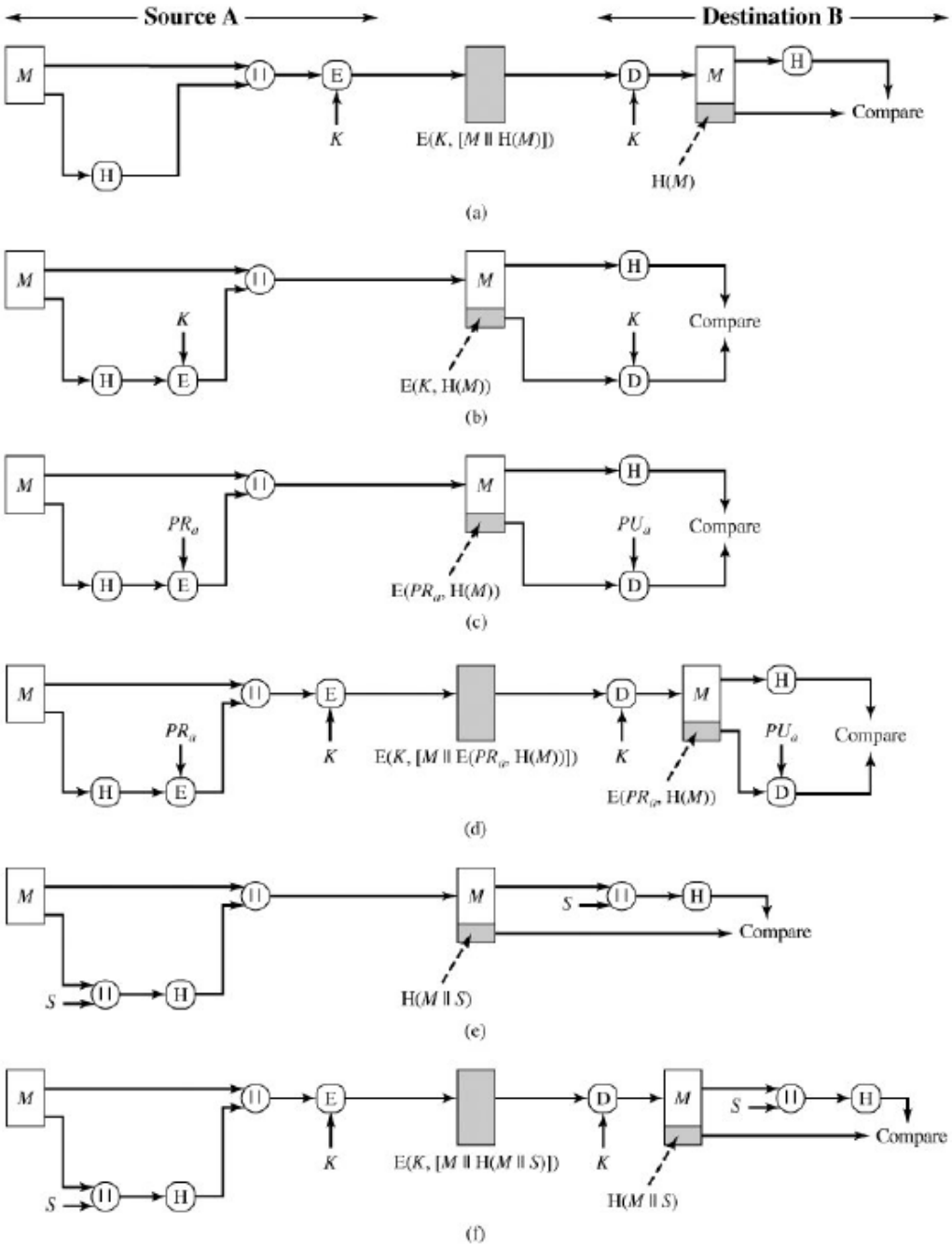

Figure 2 Basic Uses of Hash Function

Figure 2 illustrates a variety of ways in which a hash code can be used to provide message authentication, as follows:

a. The message plus concatenated hash code is encrypted using symmetric encryption.
b. Only the hash code is encrypted, using symmetric encryption.
c. Only the hash code is encrypted, using public-key encryption and using the sender's private key.

d. If confidentiality as well as a digital signature is desired, then the message plus the public-key-encrypted hash code can be encrypted using a symmetric secret key.
e. This technique uses a hash function but no encryption for message authentication. The technique assumes that the two communicating parties share a common secret value S. A computes the hash value over the concatenation of M and S and appends the resulting hash value to M. Because B possesses S, it can recompute the hash value to verify.
f. Confidentiality can be added to the approach of (e) by encrypting the entire message plus the hash code