Answer Key for CS549 End-Sem Exam 2023

Q1.

(A)

When a hash function is used to provide message authentication, the hash function value is often referred to as a **message digest**.

(B)

More commonly, message authentication is achieved using a message authentication code (MAC), also known as a **keyed hash function**.

Typically, MACs are used between **two parties that share a secret key** to authenticate information exchanged between those parties. A MAC function takes as input a secret key and a data block and produces a hash value, referred to as the MAC, which is associated with the protected message.

If the integrity of the message needs to be checked, the MAC function can be applied to the message and the result compared with the associated MAC value. An attacker who alters the message will be unable to alter the associated MAC value without knowledge of the secret key. Note that the verifying party also knows who the sending party is because no one else knows the secret key.

Anyone of the following diagrams is ok.

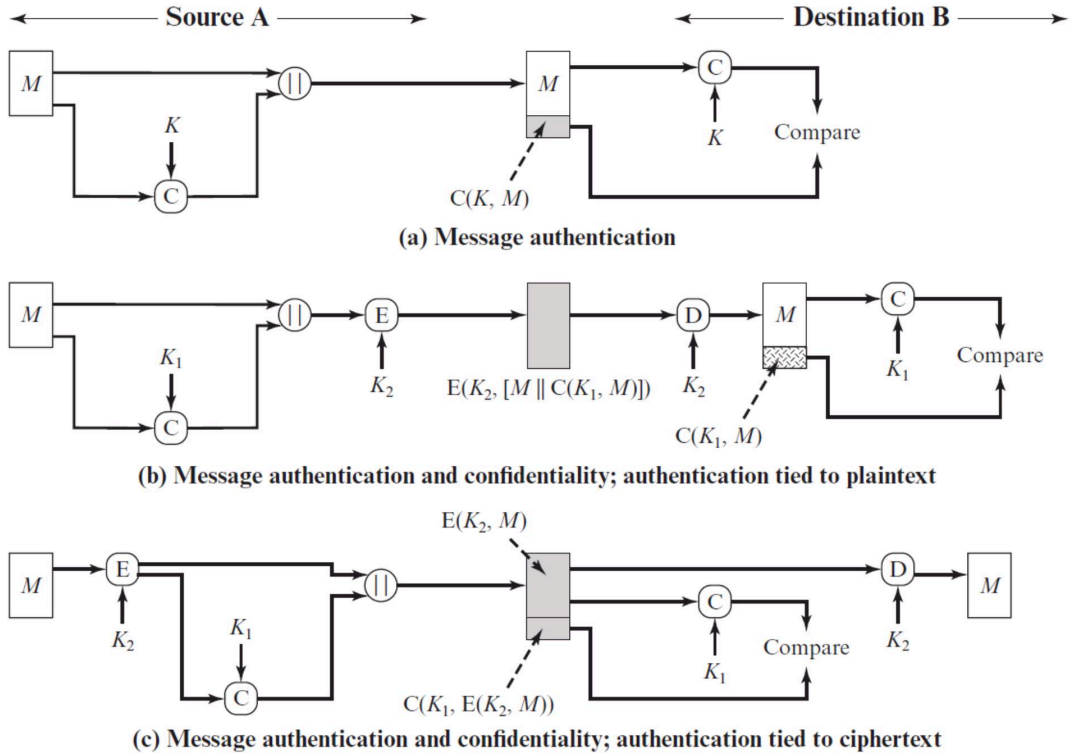


Figure 12.4 Basic Uses of Message Authentication code (MAC)

(C)

The sponge function takes an input message and partitions it into fixed-size blocks $P_0, P_1, \ldots, P_{k-1}$. Each block is processed in turn with the output of each iteration fed into the next iteration, finally producing an output block.

Figure 11.15 shows the iterated structure of the sponge function. The sponge construction operates on a state variable s of $b = r + c$ bits, which is initialized to all zeros and modified at each iteration.

This value ***r*** is the block size used to partition the input message. The value ***r*** is called the **bitrate** and the value ***c*** is referred to as the **capacity**.

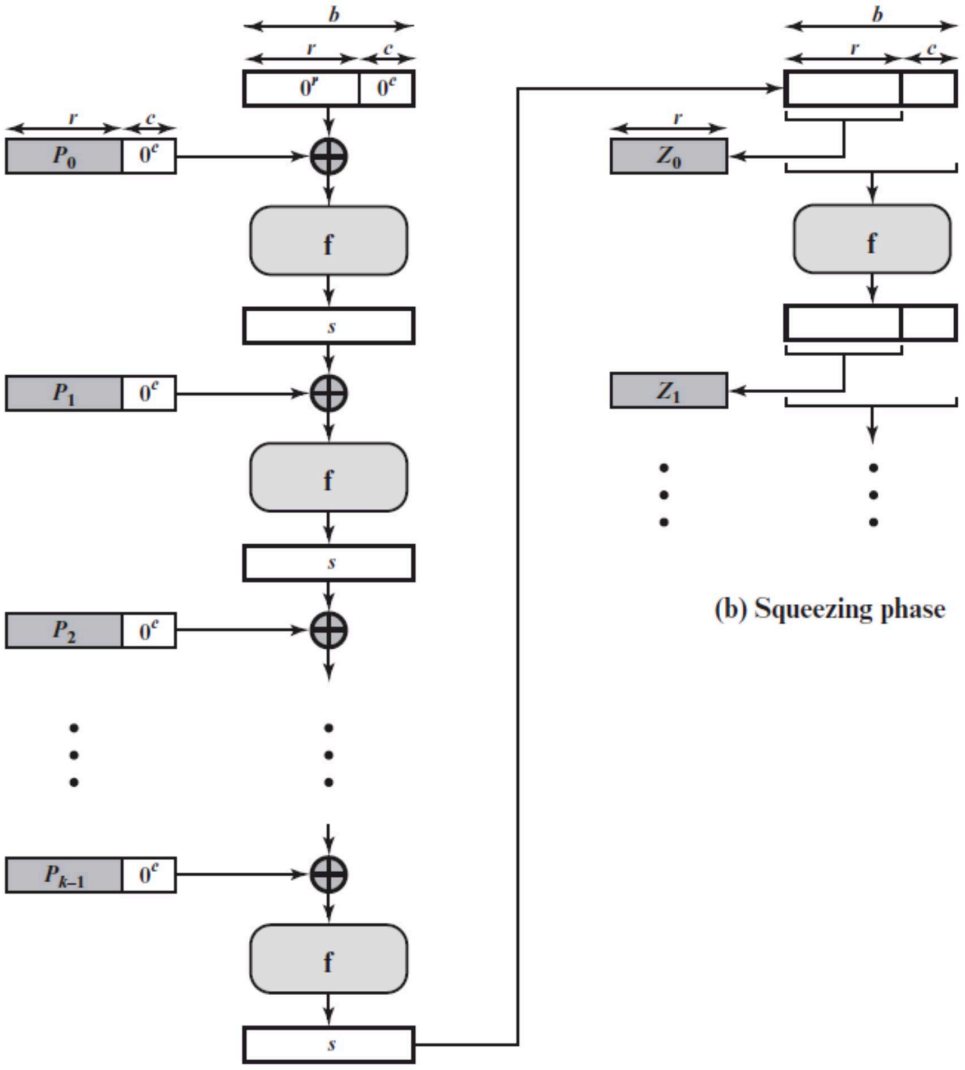


Figure 11.15 Sponge Construction

The sponge construction consists of two phases.

The **absorbing phase** proceeds as follows: For each iteration, the input block ***P*** to be processed is padded with zeroes to extend its length from ***r*** bits to ***b*** bits. Then, the bitwise XOR of the extended message block and ***s*** is formed to create a ***b***-bit input to the iteration function **f**. The output of **f** is the value of ***s*** for the next iteration.

If the desired output length ***L*** satisfies ***L*** <= ***b***, then at the completion of the absorbing phase, the first ***L*** bits of ***s*** are returned and the sponge construction terminates.

Otherwise, the sponge construction enters the **squeezing phase**. To begin, the first ***r*** bits of ***s*** are retained as block Z_0. Then, the value of ***s*** is updated with repeated executions of **f**, and at each iteration, the first ***r*** bits of ***s*** are retained as block Z_i and concatenated with previously generated blocks. The process continues through **(j - 1)** iterations until we have ***(j - 1) * r < L <= j * r***. At this point the first ***L*** bits of the concatenated block ***Z*** are returned.

Q.2

(A) Rule B allows external traffic to any destination port above 1023. So, an external attacker can open a TCP connection from the attackers port, say 5150, to an internal server, say web Proxy server running on port 8080. A simple packet filter can not ~~forbid~~ forbid such inbound TCP traffic destined to all ports >1023.

2 marks

(B) A stateful inspection packet firewall can tighten up the rules for TCP traffic by creating a directory of outbound TCP connections. The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.

3 marks

example:

Source Address	Source Port	Destination Address	Destination Port	Connection Status
192.168.1.101	1033	173.66.32.122	25	Established
223.43.21.231	1990	192.168.1.6	80	Established

Basically, the destination Address of outbound established connection will be allowed to send inbound traffic. So, attacker's system will be blocked to send inbound traffic i.e. those traffics will be discarded by the firewall.

(C) If we want to use simple packet filter firewall, we can add the source port filed in each row to deny the attacker running on port 5150. So, modified rules will be as follows:

2 marks

Rule	Direction	Source Add.	Source Port	Dest. Add.	Dest. Port	Protocol	Action
A	Out	Internal	>1023	External	25	TCP	Permit
B	In	External	25	Internal	>1023	TCP	Permit

Still the vulnerability remains. The problem with this rule is that the use of port 25 for SMTP receipt is only a default understanding. An outside machine could be configured to have some other application linked to port 25. So, an attacker could gain access to internal machines by sending packets with a TCP source port number 25.

To counter this threat, we can add ACK flag field to each row. This flag must be set on the incoming packets comming from SMTP server. This rule takes advantage of features of TCP connections. Once a connection is set up, the ACK flag of a TCP segment is set to acknowledge segments sent from the other side.

3 marks

Rule	Direction	Source Add.	Source Port	Dest. Add.	Dest. Port.	Protocol	Flag	Action
A	Out	Internal	>1023	External	25	TCP	-	Permit
B	In	External	25	Internal	>1023	TCP	ACK	Permit

Q3.

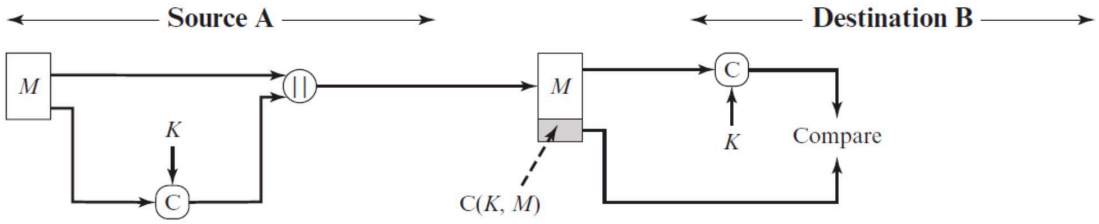
(A)

A MAC function is similar to encryption. **One difference is** that the MAC algorithm need not be reversible, but it is mandatory requirement for decryption.

So, if we assume that the required properties for MAC/Encryption are satisfied, then we can use them interchangeably for providing a required service.

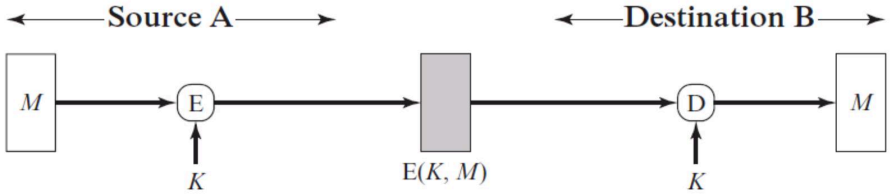
For example, message authentication can be achieved as follows.

Using MAC:



(a) Message authentication

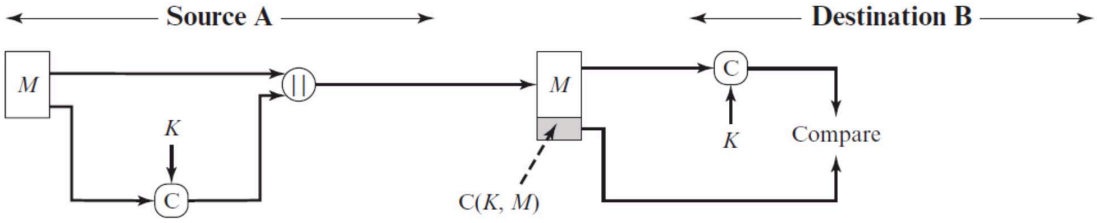
Using Encryption:



(a) Symmetric encryption: confidentiality and authentication

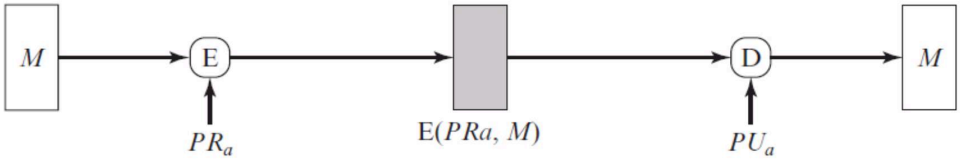
(B)

No, MAC cannot provide a digital signature, because both the sender and receiver share the same key. Hence, B cannot ensure that the received MAC has been generated and added by A only. See the following diagram:



(a) Message authentication

However, we can use public key cryptography to provide the digital signature. See the below design



(c) Public-key encryption: authentication and signature

It also provides what is known as digital signature. Only A could have constructed the ciphertext because only A possesses PR_a. Not even B, the recipient, could have constructed the ciphertext. Therefore, if B is in possession of the ciphertext, B has the means to prove that the message must have come from A. In effect, A has “signed” the message by using its private key to encrypt.

(C)

Few situations in which a message authentication code (MAC) is preferred instead of encryption for providing authentication.

1. There are a number of applications in which **the same message is broadcast to a number of destinations.** It is cheaper and more reliable to have only one destination responsible for monitoring authenticity. Thus, the message must be broadcast in plaintext with an associated message authentication code. The responsible system has the secret key and performs authentication. If a violation occurs, the other destination systems are alerted by a general alarm.
2. Another possible scenario is an exchange in which one side has a heavy load and **cannot afford the time to decrypt all incoming messages**. Authentication is carried out on a selective basis, messages being chosen at random for checking.
3. The **computer program can be executed without having to decrypt it every time**, which would be wasteful of processor resources. However, if a message authentication code were attached to the program, it could be checked whenever assurance was required of the integrity of the program.
4. For some applications, **it may not be of concern to keep messages secret, but it is important to authenticate messages.** E.g. SNMP messages
5. It may be desired to perform **authentication at the application level** but to provide **confidentiality at a lower level**, such as the transport layer.
6. With message encryption, the protection is lost when the message is decrypted, so the message is protected against fraudulent modifications only in transit **but not within the target system. MAC can provide the authentication within the system itself.**

Q4.

(A)

The heartbeat serves two purposes.

First, it assures the sender that the recipient is still alive, even though there may not have been any activity over the underlying TCP connection for a while.

Second, the heartbeat generates activity across the connection during idle periods, which avoids closure by a firewall that does not tolerate idle connections.

(B)

A TLS session is an association between a client and a server. Sessions are created by the Handshake Protocol.

Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

(C)

An SSL certificate is a digital document that mainly binds the identity of a website to a cryptographic key pair (public key & private key). An SSL certificate is a type of X.509 public key certificate, but it is a Server Certificate. It works by establishing an encrypted connection between a web browser and a server using shared secret key

(D)

Of course, one hopes that compression shrinks rather than expands the data. However, for very short blocks, it is possible, because of formatting conventions, that the compression algorithm will actually provide output that is longer than the input

(E)

Based on the Access Requestor's (AR) or Supplicant's posture and an enterprise's defined policy, the policy server determines what access should be granted. Basically, the authentication process verifies a supplicant's claimed identity, which enables the policy server to determine what access privileges, if any, the AR may have.

Q5.

(A)

Re-association service enables an established association to be transferred from one AP to another, allowing a mobile station to move from one Basic Service Set (BSS) to another.

(B)

Open system authentication: The purpose of this frame sequence, which provides no security, is simply to maintain backward compatibility with the IEEE 802.11 state machine, as implemented in existing IEEE 802.11 hardware. In essence, the two devices (STA and AP) simply exchange identifiers.

(C)

Master session key (MSK), also known as the Authentication, Authorization, and Accounting (AAA) key, is generated by the authentication server (AS) using the IEEE 802.1X protocol during the authentication phase.

All the cryptographic keys needed by the STA for secure communication with its AP are generated from this MSK if any pre-shared key (PSK) is not used.

(D)

In general, a content type declares the **general type** of data, and the sub-type specifies a **particular format** for that type of data. It describes the data contained in the body with sufficient detail that the receiving user agent can pick an appropriate agent or mechanism to represent the data to the user or otherwise deal with the data in an appropriate manner.

(E)

SMTP cannot transmit text data that includes national language characters, because these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to 7-bit ASCII.

Q6.

(A)

A believes that it shares K_S with B since its nonce N_A came back in message 2 encrypted by a key known only to B (and A).

B believes that it shares K_S with A since nonce N_A was encrypted by K_S (in message 3), which could only be retrieved from message 2 by someone who knows K_{AB} (and this is known only by A and B).

A believes that K_S is fresh since it is included in message 2 together with nonce N_A (and hence message 2 must have been constructed after message 1 was sent).

B believes (indeed, knows) that K_S is fresh since it is chosen by B.

(B)

Unfortunately, because of the nature of the probabilities involved in IDS, it is very difficult to meet the standard of high rate of detections with a low rate of false alarms. In general, if the actual numbers of intrusions is low compared to the number of legitimate uses of a system, then the false alarm rate will be high unless the test is extremely discriminating. This is an example of a phenomenon known as **base rate fallacy**.

Q7.

(A)

P=5, q=11, e=3, M=9

So, n = p*q = 55

phi(n)= (1-p)*(1-q) = 4*10 = 40

then to find d, we do the following.

d*e mod phi(n) = 1. And d < phi(n)

=> d*3 mod 40 = 1

=> d= 27

Encryption:

c= M^e mod n = 9^3 mod 55 = 729 mod 55 = 14

Decryption:

Now, M = c^d mod n = 14^27 mod 55

=> M = ((14^1 mod 55) * (14^2 mod 55) * (14^4 mod 55) * (14^4 mod 55) * (14^16 mod 55)) mod 55

Here, (14^1 mod 55) = 14 and (14^2 mod 55) = 31

So, (14^4 mod 55) = (31*31) mod 55 = 26

So, (14^8 mod 55) = (26*26) mod 55 = 16

So, (14^16 mod 55) = (16*16) mod 55 = 36

Now, M = (14 *31 * 16 *36) mod 55 = ((14*31) mod 55 * (16*36) mod 55) mod 55

=> M = (49 * 26) mod 55 = 9

(B)

(i)

By taking the first 80 bits of (v||c), Bob can obtain the initialization vector v as it was concatenated with the cipher before transmission by Alice.

Now, Bob knows the value of k as it is pre-shared.

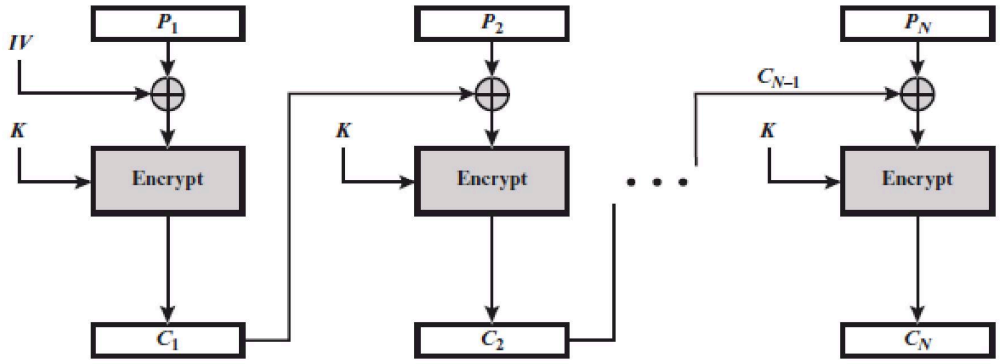
So, Bob can perform RC4(v||k) to generate the same bit stream used for encryption.

Now, if the Bob performs RC4(v||k) XOR c, then it gives the required m as RC4(v||k) XOR (RC4(v||k) XOR m)) = m. This is basically the decryption procedure.

(ii) If the adversary observes that vi = vj for distinct i, j then he/she knows that the same key stream was used to encrypt both mi and mj.

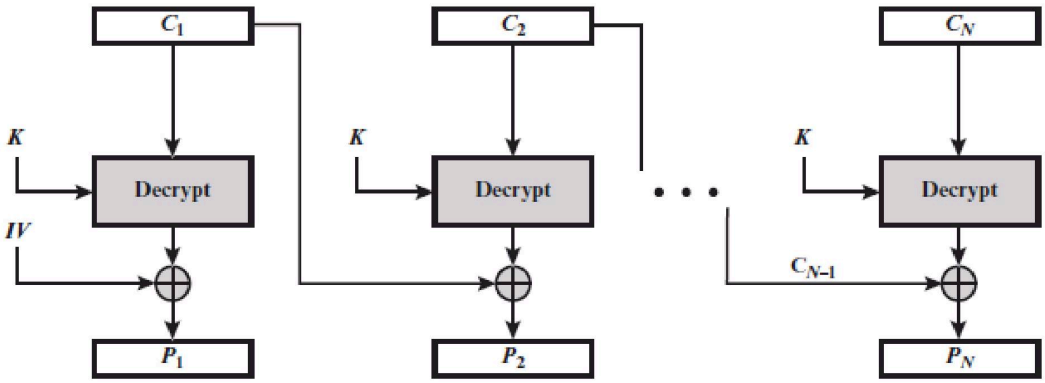
(C)

An error in P1 affects C1. Since C1 is the input to the calculation of C2, C2 is also affected. This effect carries through indefinitely, so that all ciphertext blocks are affected. See the diagram of encryption phase in CBC mode.



(a) Encryption

However, at the receiving end, the decryption algorithm restores the correct plaintext for blocks except the one in error. You can see this by writing out the equations for the decryption or in the following diagram. Therefore, the error only effects the corresponding decrypted plaintext block i.e. P1 in this case.



(b) Decryption