CSE 473 – Introduction to Computer Networks

Review Questions 24

***Your Name**:*

Please print out this form (two-sided, if you can) and write your answers *legibly* in the spaces provided. If you can't write legibly, type.

1. Explain the difference between confidentiality and integrity of messages. Can you have one without the other, and if yes, which one and why?

Confidentiality refers to the ability to transfer information without revealing it to an adversary even if the adversary intercepts it. This is typically achieved through encryption.

Integrity refers to the ability to transfer information while enabling the receiver to ensure that it has not been tampered with or corrupted. This is typically achieved by way of authentication through digital signatures computed on the information being transferred.

Integrity clearly does not imply confidentiality, i.e., adding a hash or signature of a message does not make its content unavailable to attackers. The converse may, however, in some cases hold to some extent, namely, when changing an encrypted message makes its decryption impossible, though this is clearly not true in general

2. In the block cipher shown in Figure 8.5 in the book, how many bits are needed to represent a key?

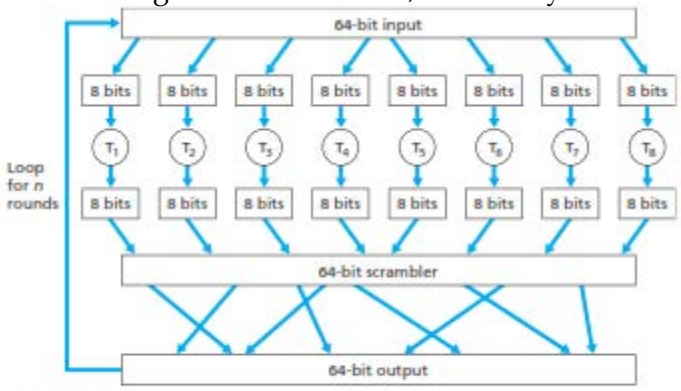

Figure 8.5 ♦ An example of a block cipher

*A key needs to encode the possible mappings/permutations that are applied to the input bits. Figure 8.5 identifies eight 8-bit mappings plus one 64 bit scrambler. One 8-bit mapping can be specified through a key of length $\lceil \log_2 2^8! \rceil = \lceil \log_2 256! \rceil = 1684$ bits. Since we have eight such tables, specifying them, if they are independent of each other, would require 8*1684=13472 bits. In addition, if the scrambler is unknown, i.e., could be arbitrarily varied to generate a coded output, we would then need a key to specify it as well. This would require an additional $\log_2 64! = 296$ bits. For a total of 13,472+296=13,768 bits.*

3. Describe two major differences between public key and secret key encryption systems, and offer an explanation for why they are often used in tandem.

   Public key encryption systems are asymmetric, i.e., the encryption and decryption keys and computations are different, while secrete key encryption systems are normally symmetric. In addition, public key encryption/decryption is typically computationally much more expensive than solutions based on secret keys. The latter is one of the reasons for using the two systems in tandem, i.e., public keys are used to select and exchange secret keys that are then used for steady-state data communications.

4. Suppose we want to construct an RSA key pair based on the initial values p=5, q=11. Is 15 an acceptable value for e? Is 27? (Ignore the fact that these values are all too small.)

   *In the above example, n=pq=55 and z=(p-1)(q-1)=40. The factor e needs to be less than n and with no common factors with z=2*2*2*5. Since 15=3*5, it fails to satisfy the second condition, while 27=3*3*3 would.*

5. What is a DNS amplification attack? Explain why and how it works, and what defense mechanisms are available to combat it.

   A DNS amplification attack leverages the availability of open DNS servers, i.e., servers that accept queries coming from any host. It involves the attacker sending a query to as many open DNS servers as possible with a spoofed source address that is that of the attack target. The combined volume of traffic coming from all the responses can overwhelm the target. To make the attack most effective, it is useful to ensure that the DNS reply is large. This can be achieved in a number of different ways. One common option is to issue a query of type ANY, i.e., for an entire zone. This ensures a large reply, but is not always supported by all DNS servers. Another option is to register a "fake" domain name and populate the entry with large text records that are to be returned with any query.

   Those attacks are difficult to protect against as the traffic is coming from legitimate DNS servers. The best options are to eliminate open DNS servers in the Internet and to ensure the implement of address filtering solutions to prevent address spoofing.