Computer Security

07r. Assignment 6 Review

Paul Krzyzanowski

TAs: Fan Zhang, Shuo Zhang

Rutgers University

Fall 2019

Question 1

What is a necessary condition for perfect secrecy?

Claude Shannon proved that a cipher has perfect secrecy if and only if there are as many possible keys as possible plaintexts, so every key is equally likely.

This means the key has to be **random** and **as long as the message** … which means that this is not practical for most real-word use cases

See page 133 of the Security Engineering text.

Question 2

How did Robert Hooke use a one-way function in 1678?

He published an anagram of a message and revealed its meaning two years later.

This allowed him to establish priority for his idea (Hooke's Law for a spring) without disclosing it at the time.

See page 137 of the Security Engineering text.

Question 2: Discussion

This is a precursor to the idea of using a *hash*.

If I publish a hash of a message, *H(M)*

… and later show you the message, *M:*

You know that I *must have had the message to generate that hash*

A good cryptographic hash function will make it difficult to generate a message that hashes to a specific, desired value

Note that “difficult” = “not feasible” = “impossible for all practical purposes”

Question 3

What are the three properties of hash functions listed in the text?

1. They are **one-way functions**
   - Given x, it is easy to compute $h(x)$ but difficult to find x when given $h(x)$

2. The function **does not give any information** about any part of the input.

3. It is hard to find **collisions**
   - A collision is when you can find two messages M_1, M_2 where $M_1 \neq M_2$ but $h(M_1) = h(M_2)$

See section 5.3.1 (Random Functions – Hash Functions), 5.3.1.1 (Properties) Page 141

Question 4

What is meant by a trapdoor one-way permutation?

"This is a computation which anyone can perform, but which can be reversed only by someone who knows a trapdoor such as a secret key. "

Public key cryptography is an example of this

– If I encrypt a message with my private key, *k*: $C = E_k(M)$

– Nobody can decrypt it without the "trapdoor", knowledge of my public key, *K*: $M = D_K(C)$

See page 147 of the text.

Question 5

How does *confusion* differ from *diffusion* in an SP network?

- **Confusion**
  - Confusion uses the key (known only to trusted parties) to modify the plaintext values (switch ones and zeros).
  - Every bit of ciphertext depends on various bits of the key. You cannot find a connection between a bit of the key and a bit of the ciphertext.
- **Diffusion**
  - The plaintext information is **spread** throughout the cipher so that a change in one bit of plaintext will affect many other bits
  - If you change a bit in the plaintext, approximately half of the bits in the ciphertext will change.

Question 6

What does an s-box do in a symmetric block cipher?

- It is a substitution box – it substitutes one pattern of bits with another
- Think of it as a lookup table
  - Example:

    Input = 1101

    Output = 1010

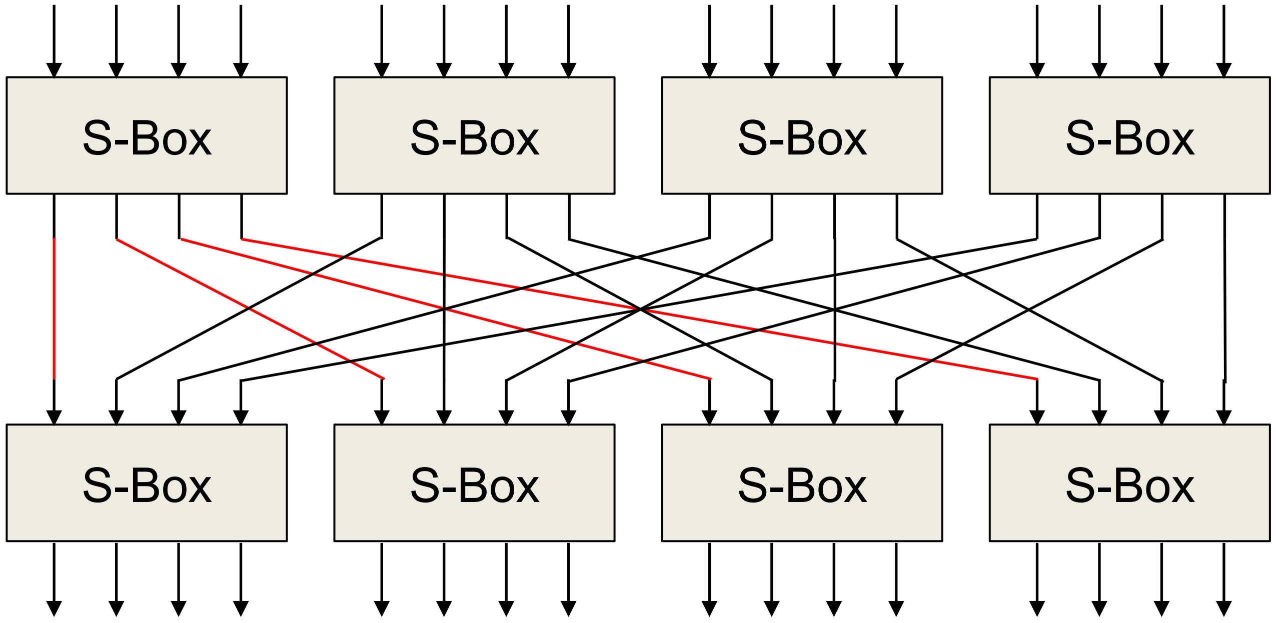
See page 5.4.1, SP Networks, p. 149 in the Security Engineering text.

6. Discussion: s-boxes

- **Block ciphers**
  - Encrypt a chunk of data at a time (rather than a byte at a time)
  - Versus stream ciphers, which encrypt one byte at a type
  - Essentially all symmetric block ciphers use SP Networks
- General goal: *Confusion and Diffusion*
  - Confusion = key hides the relationship between any bit of the plaintext input and any corresponding bit of the ciphertext output
  - Diffusion = spread plaintext data throughout ciphertext block
- SP Networks: <u>substitution</u> and <u>permutation</u>
  - Used in implementing block ciphers
  - S-box = lookup table that maps a set of bits onto another set
  - Some bits of the key may select which s-box to use
  - … or some bits of the key might be used as input to the s-box

6. Discussion: s-boxes

- Encryption involves multiple rounds
  - The output of one set of s-box operations is used as input to the next round
- A simple 16-bit, 2-round SP-network from the text (p. 151):



The end