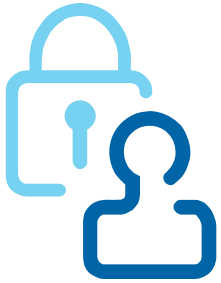
Security and Authentication



2020

Tutorials 1 – Week 1

Revision

- **What is the difference between a block cipher and a stream cipher?**
  - A stream cipher process one input element at a time. The block cipher process a block of elements at a time.
- **What is the purpose of the S-box in DES? How is it used? Explain.**
  - The S-box (substitution box) is used to perform substitution on the message contents.
  - The purpose is to 'confuse' the information of the original message.
  - It consists of a table (4 X 16) where the entries of the table are the substitution values.
  - The first and last bits from a 6-bits block are used to represent a binary number and refer to a row on the table. The remaining 2 to 5 bits form a binary number to refer to a column in the table.
  - The overlap between the selected row and column holds the new value which the S-box is going to use in the substitution.

Revision

- **How does a one-time pad work and how secure it is?**
  - A one time pad is a stream cipher that it is unbreakable.
  - For each message a new random key is used, where the key is the same size as the message.
  - Encryption produces a random output that has no statistical relationship to the plaintext.
  - **Weaknesses**: easy to implement wrongly.

- **What is cryptography?**
  - Cryptography is the art of secret writing, is the process of converting information that can be read by most, into a secret code, that can only be read by those who are party of the secret.

1. Briefly explain the security services of confidentiality, integrity and availability.

Solution key:

Confidentiality: preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorised disclosure of information.

Integrity: guarding against improper information modification or destruction. A loss of integrity is the unauthorised modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

2. Consider a student attendance information system in which the students provide a password for accessing their accounts. Give examples of the security services the system should provide in terms of confidentiality, integrity, access control and availability.

Solution key:

The system must keep all passwords and account information confidential, both in the server and during the transaction.

It must protect the integrity of data records from unauthorised changes.

It must also limit access of various levels of data to the right users only; e.g. students can only access their own information, and instructors can access all students attendance records.

Availability of the server during the college working hours is important, and needs to withstand DoS attacks.

3. Why is Caesar cipher substitution technique vulnerable to a brute-force cryptanalysis?

Solution key:

There are only 25 keys to try – very easy.

4. Why is the one-time pad scheme unbreakable? What are the practical problems of one-time pad?

Solution key:

Given a certain ciphertext, there are keys that produces different plaintext. If you did an exhaustive search of all possible keys, you would end up with many legible plaintexts, with no way of knowing which was the intended plaintext. The ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

The key size is as big as the message, so can have limitations.

It is also easy to get wrong.

5. Construct a Playfair matrix with the key ***reason***. Make a reasonable assumption about how to treat redundant letters in the key. Encrypt the message: **See some light in the darkness**.

Solution key:

Matrix:

R	E	A	S	O
N	B	C	D	F
G	H	I/J	K	L
M	P	Q	T	U
V	W	X	Y	Z

SE ES OM EL IG HT IN TH ED AR KN ES SX

Cipher text: OA AO RU OH KH KP GC PK SB SE GD AO AY

6. Using Vigenere Cipher, encrypt the word "**examination**" using the key "***grades***".

Solution key:

key:	g r a d e s g r a d e
plaintext:	e x a m i n a t i o n
ciphertext:	KOAPMFGKIRR

7. Briefly define the terms **substitution** and **permutation**.

Solution key:

In *substitution*, each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.

In *permutation*, a sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.

8. Which are the two main areas of concern related to the level of security provided by DES?

Solution key:

The two main areas of concern related to the level of security provided by DES are: key size and the nature of the algorithm, e.g. the design of S boxes and the choice of specific permutations.

9. What is the purpose of the key expansion algorithm used in AES?

Solution key:

The AES key is 4 words (128 bits), which is used for round 0. For round 1 – 10, the key expansion algorithm provides a new 4-word round key for each of the 10 rounds.

10. A typical round of AES encryption consists of four stages (Substitution bytes, Shift Rows, Mix Columns and Add Round Key). Describe the functionality of each stage.

Solution key:

Substitute Bytes: Uses an S-box to perform block substitutions. Each of the 'state' bytes is split into two 4-bit values; these represent the column and row values of the S-box containing the new substitution value.

Shift Rows: A simple permutation where the 'state' block is altered by re-arranging the bytes located on each of the four rows.

Mix Columns: A substitution that makes used of arithmetic over GF(2^8). Hence, each of the 'state' elements is updated using the product of elements of one row and one column.

Add Round Key: A simple bitwise XOR of the current block with a portion of the expanded key. The expanded key is obtained through the 'expansion algorithm'.

- When PT109 was sunk by a Japanese destroyer in WWII (this was JFK's command), the following message was received at an Australian monitoring station in Playfair code:

KX JEY UREBE ZWEHE WRYTU HEYFS

KREHE GOYFE WTTTU OLKSY CA JPO

BOTE I ZONTX BYBWT GONEY CUZWR

GDSON SXBOU YWRHE BAAHY USEDQ

- The key is *royal new zealand navy*: decrypt the message.

Solution

- Sort the key
  - ROYAL NEW ZEALAND NAVY
  - **ROYALNEWZDV**
- Place in block and fill the remaining alphabets:

KX JEY UREBE ZWEHE WRYTU HEYFS
KREHE GOYFE WTTTU OLKSY CAJPO
BOTE I ZONTX BYBWT GONEY CUZWR
GDSON SXBOU YWRHE BAAHY USEDQ

PT BOAT ONE OWE NINE LOST IN ACT
ION IN BLACNETT STRAIT TWO MIL
ES SW MERESU COCE X CREW OF TWEL
VE X REQUEST ANY INFORMATION X

R	O	Y	A	L
N	E	W	Z	D
V	B	C	F	G
H	I/J	K	M	P
Q	S	T	U	X

PT BOAT ONE OWE NINE LOST IN ACTION IN BLACNETT STRAIT TWO MILES SW MERESU COCE X CREW OF TWELVE X REQUEST ANY INFORMATION.