IS53012C Security and Encryption

Dr Ida Pu

Goldsmiths, University of London

2022←2007

Portfolio **Read Me**

- Your portfolio should include the answers to at least the following questions, ideally in a single .pdf file.
- Answers to questions of other weekly exercise or homework are encouraged to submit without credit.
- If it is a group work, please include a cover sheet including 1. justification of the group work, 2. full names of all the group members, and 3. their roles in terms of Alice, Bob and Charlie. Each group should submit ONE portfolio only by Alice (Bob if there is no Alice).
- Questions often correspond to contents covered in the same week. You should therefore study lect1_4pp.pdf–lectN_4pp.pdf *before* answering any questions in WeekN, where N is the week number.

Week 1

1. Consider each of the following attacks and discuss which aspects of the Computer Security have been threatened.
   (a) Equipment is stolen
   (b) An unauthorised copy of software is made
   (c) Existing files are modified
   (d) Messages are destroyed
   (e) Traffic patterns of messages are observed

Week 1 (continued)

2. Given the probability distributions of two event sources $P_1 = [0.3, 0.2, 0.4, 0.1]$, and $P_2 = [0.3, 0.1, 0.5, 0.1]$, which source is more random on average? Justify your answer.
3. What can you say about a binary source with two events only?
   Hint: Plot the entropy against the binary probability distribution.

Week 2

John proposes a cryptosystem that is based on one-time key pad and requires no key exchange. It works as follows: If she wants to send Bob a message m, Alice generates her key k_a, a sequence of random bits (the same length as m), computes $c = m \oplus k_a$ and sends c to Bob, where $\oplus$ represents the bitwise XOR operation. On receipt of c, Bob generates his own random bits k_b of same length, computes $d = c \oplus k_b$ and sends d to Alice. On receipt of d, Alice computes $e = d \oplus k_a$ and sends e to Bob. On receipt of e, Bob computes $e \oplus k_b$ for the last time.

Analyse John's cryptosystem and conclude whether John's cryptosystem works.

Week 2 (continued)

The following format may be adopted to help demonstrate what happens with the plaintext m that from Alice to Bob, where "??" parts are for you to figure out. Each of the 3 columns shows the series of the values (or texts) visible by Alice, Bob or Charlie.

$$\begin{tikzcd}
\text{Alice} & \text{Charlie} & \text{Bob} \\
m \arrow[d] & & \\
?? \arrow[r] & ?? \arrow[r] & ?? \arrow[d] \\
?? \arrow[d] & ?? \arrow[l] \arrow[d] & ?? \arrow[l] \\
?? \arrow[d] & ?? & \\
?? \arrow[r] & ?? \arrow[r] \arrow[d] & ?? \arrow[d] \\
 & ?? & ??
\end{tikzcd}$$

Week 3

2. Let the password seed be 1101 which is known by both Alice and Bob.
   (a) Demonstrate how Alice and Bob can independently generate an identical new random password of up to 15 bits without sending the new password.
   (b) What are the risks?

Week 4

4. Demonstrate how the Vernam cipher works for the example of plaintext "computer" and the one-time pad (5 20 0 9 17 16 22 18). Explain why the cipher is hopeless in practice.
5. Explain how the transposition cipher works. Demonstrate how the plaintext can be decrypted from the ciphertext HKFPRZNIWUVLG UOJOEO TCNMEAOEBOETYCQRXDHDE, using the key IAMTHE.
6. Consider the RSA (Rivest, Shamir and Adleman) cryptosystem. Before sending a message $m = 3$ to Alice, Bob prepares his keys carefully. He randomly chooses $p = 5$, $q = 7$ and $e = 7$. Answer the following questions on the RSA cryptosystem. Show all your work.
   (a) What is the value of n, the RSA modulus?
   (b) What is the value of $r = \varphi(n)$?
   (c) What is the value of the decryption exponent d?
   (d) Which values are used as Bob's *private key*?
   (e) Which values are used as Bob's *public key*?

Week 5

If g is a generator for prime p, then the value of $g^n \mod p$ is a different value for every $n \in [1, p-1]$.

1. Show $g = 3$ is a generator for $p = 17$.
2. Show $g = 2$ is not a generator for $p = 17$.

[Hints]

n	1	2	$\cdots$	$p-1$
$g^n \mod p$			$\cdots$	

Week 7

Let L be the *power set* of (a,b,c). The system low is $\emptyset$ and the system high is (a, b, c). Draw the lattice for $(L, \subset)$.

Week 8

Discuss the sensitivity of each of the following disclosures and explain why.

i. The sum of all financial supports for students in our department.

ii. A list of students receiving financial supports in our department.

iii. Charlie got the above sum in January and the list in October.

iv. What computation would a database management system have to perform in order to determine that the list of names might reveal sensitive data?

Portfolio **Mark Scheme**

A total of 30 marks:
week 1 [3x2]
week 2 [3]
week 3 [3]
week 4 [3x3]
week 5 [3]
week 7 [3]
week 8 [3]