ISEC2000 Fundamental Concepts of Cryptography
Final Assessment, 2022
@ Computing, Curtin University

Timing:
You have **2 hours 15 minutes** to complete the assessment.

Weighting:
This assessment contains 9 questions, for a total of 100 points, which weights for 50% of the final mark.

Submission:
You should submit **a single PDF** file to Blackboard e-Test and Turnitin. You can include screenshots or photos in your pdf, but make sure they are clear. Name the file as `<studentID>_<name>_exam.pdf`. Use the `Declaration_of_originality.pdf` as the cover page.

Academic Integrity:
This is an **individual** assignment so that any form of collaboration is not permitted. This is an **open-book** assessment. You are free to use lecture slides, notes or any other written materials but **online search (e.g., Google) is prohibited**. It is your responsibility to understand Curtin's Academic Misconduct Rules, for example, post assessment questions online and ask for answers is considered as contract cheating and not permitted.

1. (10 points) Discuss the difference between practical security (aka computational security) and theoretical security (aka unconditional security, perfect secrecy). How to achieve perfect secrecy?

2. (10 points) Discuss how does redundancy coding help detect and correct error bits in telecommunication.

3. (10 points) Considering the following stream cipher in Fig.1 with a Linear Feedback Shift Register (LFSR) as the random key generator. The initial state of the LFSR is given as $key = (k_0, k_1, k_2, k_3) = (1100)$. For a plaintext message $m = \underline{1}0101010$ (the bit underlined is the first bit), compute the corresponding ciphertext step-by-step.

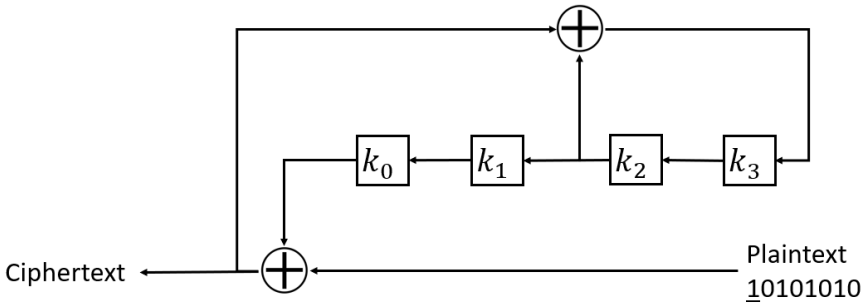

Figure 1: A stream cipher with a LFSR as the random number generator.

4. (10 points) In the DES, one of the s-boxes is given as below: Given an

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

input stream (110011) please show what is the output binary stream step-by-step.

5. (12 points) Show that the Feistel structure in DES is reversible.

6. (12 points) Considering the RSA cipher with the configuration of $p = 3$, $q = 5$, $e = 3$,
   (a) Compute the private key d. Show your derivation.
   (b) For a message $m = 21$, show the process of encryption and decryption.

7. (12 points) Describe the Diffie-Hellman Key Exchange protocol and explain its weakness to man-in-the-middle attack, with the help of the protocol diagram.

8. (12 points) Suppose $h(m)$ is a collision resistant hash function that maps a message of arbitrary bit length into an 256-bit hash value. Assume the best know attack is brute-force attack and an attacker can perform 2^{32} hashes per second
   (a) Given a particular message m_1, how long does it take to find another message m_2 such that $h(m_1) = h(m_2)$?
   (b) How long does it take for an attacker to find a random collision, i.e., $h(m_1) = h(m_2)$ for arbitrary messages m_1, m_2?

9. (12 points) Discuss the similarity and difference between message hash, message authentication code, and digital signature.

END OF ASSESSMENT