University of New Brunswick
Faculty of Computer Science
CS4355/6355: Cryptanalysis and DB Security
Theory Homework Assignment 1, ***Due Time, Date*** *5:00 PM, October 31, 2019*

Student Name: ____________________________ Matriculation Number: ________________

Instructor: Rongxing Lu
The marking scheme is shown in the left margin and [100] constitutes full marks.

[**30**] 1. Please answer the following questions.

[5] (a) List and briefly define categories of passive and active security attacks.

[5] (b) List and briefly define the basic security requirements in computer and network security.

[5] (c) Describe the Kerckhoffs Principles.

[5] (d) Describe the functions of confusion and diffusion in symmetric ciphers.

[5] (e) Describe the Strict Avalanche Conditions in symmetric ciphers.

[5] (f) Describe the key management problem in conventional cryptosystems.

[**5**] 2. A fundamental cryptographic principle states that all messages must have redundancy. But we also know that redundancy helps an intruder tell if a guessed key is correct. Consider two forms of redundancy. First, the initial n bits of the plaintext contain a known pattern. Second, the final n bits of the message contain a hash over the message. From a security point of view, are these two equivalent? Discuss your answer.

[**5**] 3. Suppose that a message has been encrypted using DES in ciphertext block chaining mode. One bit of ciphertext in block C_i is accidentally transformed from a 0 to a 1 during transmission. How much plaintext will be garbled as a result?

[**10**] 4. The following is a ciphertext with Caesar Cipher, please analyze it, and give the corresponding plaintext and the used key.

DRO MSDI LBSWC GSDR CEWWOB'C NOVSQRDC, GSDR MYVVBPEV ZBYNEMO SX DRO WKBUOD CDKXNC KXN RKGKSSKX WECSM CZSVVSXQ YXDY LOKMROC.

[**6**] 5. Please complete the following two tables, and describe why Z_{11} and Z_{11}^* are abelian groups.

$z = x + y\ mod 11$		x										
		0	1	2	3	4	5	6	7	8	9	10
y	0											
	1											
	2											
	3											
	4											
	5											
	6											
	7											
	8											
	9											
	10											

$z = x \times y\ mod 11$		x									
		1	2	3	4	5	6	7	8	9	10
y	1										
	2										
	3										
	4										
	5										
	6										
	7										
	8										
	9										
	10										

[**6**] 6. Prove the following:

[3] (a) $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$

[3] (b) $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

[**12**] 7. Prove the following:

[4] (a) Prove the One-time padding is provably secure.

[4] (b) Prove the Fermat's Little Theorem $a^{p-1} \equiv 1 \bmod p$, where p is prime and $\gcd(a, p) = 1$.

[4] (c) Prove that there are infinitely many primes.

[**6**] 8. Using the extended Euclidean algorithm, find the multiplicative inverse of

[3] (a) $1234 \bmod 4321$

[3] (b) $550 \bmod 1769$

[**20**] 9. Suppose Alice and Bob share the common modulus $n = p \times q = 35263$, but have different public-private key pairs $(e_1 = 17, d_1)$ and $(e_2 = 23, d_2)$. If David wants to send a message M to Alice and Bob, he first computes the cipher text $C_1 = M^{e_1} \bmod n$ for Alice, the value of C_1 is 28657, and also computes the cipher text $C_2 = M^{e_2} \bmod n$ for Bob, the value of C_2 is 22520. Finally, David sends (C_1, C_2) to Alice and Bob, respectively. Now, suppose a passive adversary A eavesdrops the ciphertexts (C_1, C_2). Can the adversary A recover message M just from (C_1, C_2) and the public keys (n, e_1, e_2)? If the adversary A can, please show what strategy that the adversary A would apply, and give the value of message M as well.