Student name:

Last 4 digits of student ID:

Test 1

1) This question deals with Confidentiality, Integrity, and Availability (CIA).

1a) Define each of the terms Confidentiality, Integrity, and Availability.

1b) Give a concrete example where Confidentiality is more important than Integrity.

1c) Give a concrete example where Integrity is more important than Confidentiality.

1d) Give a concrete example where Availability is the overriding concern.

2) Draw a line between each crypto term on the left and one characteristic on the right.

Term	Definition
Cryptanalysis	The making of “secret codes.”
Cryptography	The breaking of “secret codes.”
Symmetric Key Crypto	Inner workings of a cryptosystem are known.
Public Key Crypto	Same key for encryption and decryption.
Kerckhoff’s Principle	Different keys for encryption and decryption.
Plaintext	Configures a cryptosystem for encrypt/decrypt.
Ciphertext	The result of decryption.
Key	The result of encryption.

3) This question deals with the "shift-by-n" and "permutation" implementations of a Simple Substitution Cipher. These implementations are constrained to the UPPERCASE English alphabet and therefore are formally known as mono-alphabetic substitution ciphers.

3a) How many possible keys exist in a "shift-by-n" implementation?

3b) How many possible keys exist in a "permutation" implementation?

3c) Encrypt the plaintext `BREECHDETECTED` using Caesar's Cipher ("shift-by-n" where n=3)

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

3d) Decrypt the ciphertext `IBRLDGBRKGZMVNYQ` using the permutation implementation.

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

3e) While a "permutation" implementation drastically increases the number of possible of keys when compared to a "shift-by-n" implementation, both implementations are not secure. Describe an attack against simple substitution ciphers that avoids an exhaustive key search.

4) Check all that apply to our "Definition of Secure" and ciphers in general.

[ ] The best-known attack on a cipher system requires as much work as an exhaustive key search.

[ ] A cipher can never offer more security than an exhaustive key search.

[ ] Provably secure ciphers are plentiful and practical for most uses.

[ ] The size of the key is considered a cipher's "advertised" security.

5) Consider the One-Time Pad, the only provably secure cryptosystem we covered.

5a) Check all the statements that apply to the One-Time Pad.

[ ] The One-Time Pad key is a string of random bits that is the same length as the plaintext.

[ ] One-Time Pad keys may be reused multiple times.

[ ] Encryption is performed by XORing the key with the plaintext.

[ ] Decryption is performed by XORing the ciphertext with the key.

[ ] The One-Time Pad cryptosystem is practical for high data-rate systems.

5b) This question deals with encryption and decryption using the One-Time Pad.

Assume the following alphabet:

Letter	C	D	E	L	P	O	S	Y
Binary	000	001	010	011	100	101	110	111

Encrypt the plaintext `DEPLOYDECOYS` using the supplied One-Time Pad key:

Plaintext	D	E	P	L	O	Y	D	E	C	O	Y	S
	001	010	100	011	101	111	001	010	000	101	111	110
Key	101	001	111	110	001	010	101	110	100	011	111	010
Ciphertext	100											
	P											

Decrypt the ciphertext `OEECLPDDOSYP` using the supplied One-Time Pad key:

Ciphertext	O	E	E	C	L	P	D	D	O	S	Y	P
	101	010	010	000	011	100	001	001	101	110	111	100
Key	101	001	111	110	001	010	101	110	100	011	111	010
Plaintext	000											
	C											

6) Recall that Classic Codebook ciphers use codebooks to define numeric or alphabetic substitutions for words or phrases. Since the security of codebooks relied on the physical books themselves, additive sequences were adopted to extend the life of codebooks.

Using the following excerpt from a decryption codebook:

167	person
220	anything
531	tried
312	never
244	a
417	mistake
613	who
139	made
443	new

Decrypt the ciphertext:

711, 499, 858, 743, 298, 482, 574, 689, 758, 353, 706

assuming the following additive sequence was used:

467, 332, 245, 431, 159, 238, 157, 377, 227, 133, 263

Plaintext:

7) Check all the statements that apply to Stream Ciphers:

[ ] A Stream Cipher takes a key K of *n* bits in length and stretches it into a long keystream.

[ ] The keystream generated by a Stream Cipher needs to be as long as the plaintext.

[ ] Since a stream cipher is based on the One-Time Pad, it is also provably secure.

[ ] To encrypt using a Stream Cipher, XOR the plaintext with the keystream.

[ ] To decrypt using a Stream Cipher, XOR the ciphertext with the keystream.

[ ] In a Stream Cipher, different keystreams are used for encryption and decryption.

8) This question deals with the A5/1 Stream Cipher. The A5/1 stream cipher was designed to run in hardware and therefore employs LFSRs (Linear Feedback Shift Registers).

Recall the A5/1 algorithm for generating keystream bits:

At each step: $m = \text{maj}(x_8, y_{10}, z_{10})$
- Examples: $\text{maj}(0,1,0) = 0$ and $\text{maj}(1,1,0) = 1$

If $x_8 = m$ then X *steps*
- $t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$
- $x_i = x_{i-1}$ for $i = 18,17,\ldots,1$ and $x_0 = t$

If $y_{10} = m$ then Y *steps*
- $t = y_{20} \oplus y_{21}$
- $y_i = y_{i-1}$ for $i = 21,20,\ldots,1$ and $y_0 = t$

If $z_{10} = m$ then Z *steps*
- $t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22}$
- $z_i = z_{i-1}$ for $i = 22,21,\ldots,1$ and $z_0 = t$

Keystream bit is $x_{18} \oplus y_{21} \oplus z_{22}$

Assuming the following initial fill for registers X, Y, and Z:

1	0	1	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	1
X_0	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}

0	1	0	1	1	0	0	0	1	1	0	0	0	1	1	1	0	0	1	0	0	0
Y_0	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}	Y_{17}	Y_{18}	Y_{19}	Y_{20}	Y_{21}

1	1	0	0	1	1	0	1	0	0	1	0	1	0	1	0	0	0	1	1	0	1	0
Z_0	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7	Z_8	Z_9	Z_{10}	Z_{11}	Z_{12}	Z_{13}	Z_{14}	Z_{15}	Z_{16}	Z_{17}	Z_{18}	Z_{19}	Z_{20}	Z_{21}	Z_{22}

List the first two keystream bits that would be generated by A5/1 (show your work):

9) Check all the statements that apply to *Fiestel* Block Ciphers:

[ ] The plaintext is split into fixed-size blocks and fixed-size ciphertext blocks are produced.

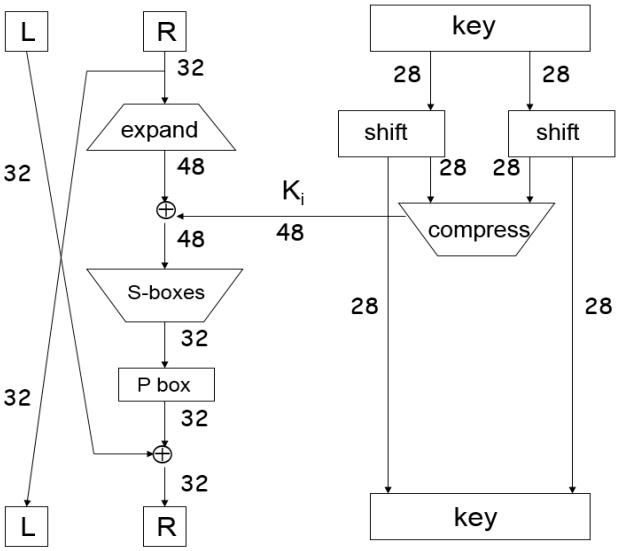
[ ] Ciphertext blocks are obtained by iterating a round function F for some number of rounds.

[ ] The input to the round function F is the key and the output of the previous round.

[ ] Due to XOR, the round function F does not need to be invertible, but non-trivial.

[ ] In a Fiestel cipher different logic is used to encrypt versus decrypt.

10) The following question deals with the DES (Data Encryption Standard) block cipher.



Explain at a *high level* what occurs in one round of DES. You may explain using a sequence of events or pseudocode, whichever you prefer. Note: Ignore *how* K_i is generated by the key scheduler on the right half of the diagram.

11) This question deals with DES and Triple DES. Even though no attacks exist against DES, its relatively small keyspace of 2^{56} possible keys is susceptible to exhaustive search. Triple DES increases the keyspace to 2^{112} possible keys while providing backwards compatibility with DES.

Recall that the general notation for encryption using a block cipher is C = E(P, K) where C is the ciphertext, E is encrypt, P is the plaintext, and K is the key.

Recall that the general notation for decryption using a block cipher is P = D(C, K) where P is the plaintext, D is decrypt, C is the ciphertext, and K is the key.

Recall that Triple DES (despite its name), uses 2 Keys K_1 and K_2.

11a) Write notation for encryption using Triple DES:

11b) Write notation for decryption using Triple DES:

11c) To demonstrate backwards compatibility of Triple DES with DES, write notation for decrypting ciphertext using Triple DES that was encrypted using DES.

12) Consider the Block Cipher Modes ECB, CBC, and CTR covered in the text and lecture.

12a) Draw line(s) between each Mode on the left and characteristic(s) on the right.

Mode	Characteristic
	Chain blocks together for improved security.
ECB	Most efficient for overwriting ciphertext blocks.
	Encrypt each block independently.
CTR	Block cipher acting like a stream cipher.
	Same plaintext yields same ciphertext (serious weakness).
CBC	Similar to a codebook with an additive.
	Can used to compute a MAC for verifying integrity.

12b) ECB mode has a weakness where identical plaintext can yield identical ciphertext (recall the picture of Alice). Explain why CBC mode does not have this weakness.

13) Check all the statements that apply to Public Key Cryptography.

[ ] A public key can be used to encrypt messages for the owner of the private key.

[ ] A private key can be used to digitally sign a message.

[ ] A public key can be used to verify a digital signature.

[ ] Signing a message with the private key ensures we know who the sender is.

[ ] In addition to non-repudiation, a digital signature can also provide integrity.

[ ] Signing a message provides confidentiality (prevents unauthorized reading).

14) This question deals with RSA encryption and decryption. Recall that an RSA public key consists of the modulus N and encryption exponent *e*. The private key consists of decryption exponent *d*.

14a) Encrypt the message M using the information in the table below:

Public key (N, e)	(33, 3)
Message M	14
$C = M^e \bmod N$	

14b) Decrypt the ciphertext C using the information in the table below:

Public key (N, e)	(33, 3)
Private key d	7
Ciphertext C	5
$M = C^d \bmod N$	

15) To speed up RSA encryption, we can make encryption easy by selecting a small encryption exponent *e* (decryption remains expensive). When *e*=3 we are vulnerable to an attack. Which one? How can we prevent the attack?