COMP435 Written Assignment 2 Name: _____

Question 1: Kerkhoff's Principle Kerckhoffs' principle states that an encryption scheme (including encryp- tion and decryption algorithms, key generation process, and key management protocol) should not have to remain secret; the encryption scheme should remain secure even if the attacker knows the scheme, as long as the attacker does not know the secret key. Explain why this is important (provide 2 reasons):

1.1. Reason 1

1.2. Reason 2

Question 2: One-Time Pad Whitney and Colleen communicate using a one-time pad and using modular arithmetic of alphabetic symbols (e.g., "a" + "b" = "a" + 2 = "c"). Whitney sends Colleen the following ciphertext (spaces, capitalization, and punctuation are removed during encryption): "elbdqirelbhdqiawsireq". An attacker sees this ciphertext and also manages to find out through social engineering that the first word of the original plaintext is "agreed".

2.1. The attacker can use this knowledge to recover the first 6 symbols of the key material (True/-False)

2.2. The attacker can use this knowledge plus knowledge of frequency patterns in English to recover the entire original plaintext with high probability. (True/False)

2.3. The attacker can use this knowledge to encrypt and send the message "agreed" to Colleen at a later date and Colleen will believe it came from Whitney. (True/False)

Question 3: Guessing a Key Now Colleen and Whitney are using AES to encrypt their communication. An attacker has been watching their communication and would like to recover the shared 128-bit key that they use. If the attacker can try 10^{15} keys per sec, approximately how many years will it take on average for the attacker to find the key? Use approximations and do this by hand. Assume there are 3×10^7 seconds in a year. You can leave your final answer in scientific notation. Show your work. (Hint: $2^{10} \approx 10^3$... and so on!)

Question 4: Passwords for Authentication! List one reason why passwords are....

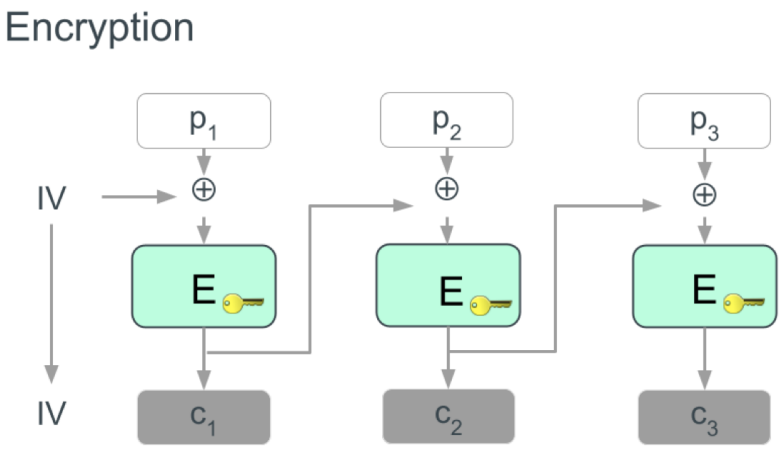
4.1. a good choice for authentication

4.2. a bad choice for authentication

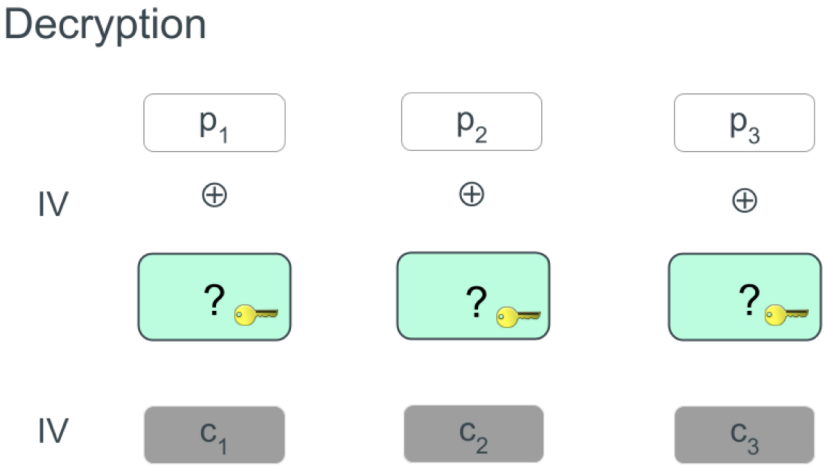
Question 5: Password Requirements Websites often require users to choose a password that contains at least one upper case letter, one lower case letter, one number, and one special character. This is done to (choose one)

- ◯ Make the set of possible passwords larger, thereby making it harder for an attacker to guess
- ◯ Encourage a more uniform distribution of passwords chosen from the set of possible passwords
- ◯ Make the passwords easier for the user to remember so they will be less likely to write them down
- ◯ Frustrate the user and discourage people from using the site

Question 6: Block Ciphers 6.1. Which block cipher mode is illustrated in the following figure?



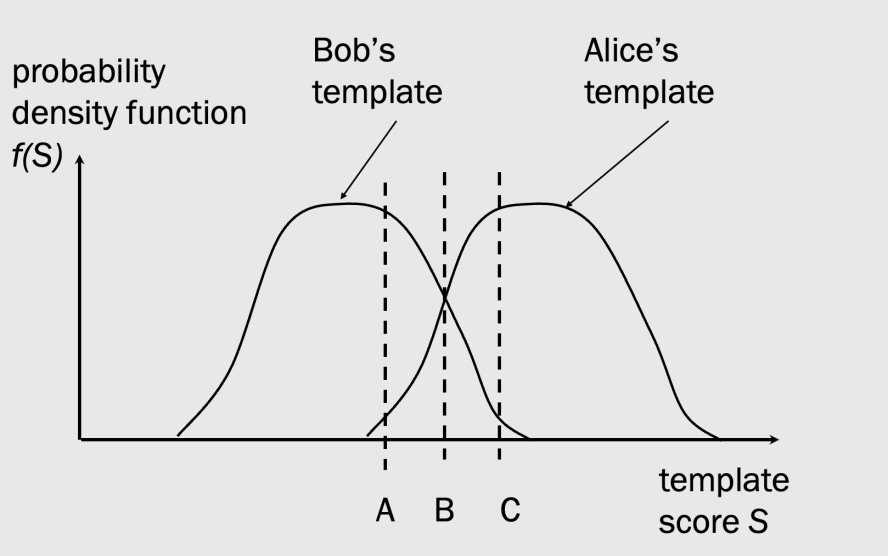
6.2. The following figure is showing the decryption algorithm for the same block cipher mode. Complete the diagram by drawing in all the missing arrows and indicating whether block **encryption** or block **decryption** is needed. Be sure to draw clearly.



Question 7: Biometrics Security Which one of the following situations is using Biometrics in the most secure way?

- ◯ Facial recognition software for logging in to a remote server. A user shows their face to their laptop camera, the image is forwarded to the server, and the server authenticates the user.
- ◯ Facial recognition software for logging on to a laptop. A user shows their face to the laptop camera, and the laptop authenticates the user.
- ◯ A fingerprint reader at the door to an office building. Users must first show ID to a guard and then use the fingerprint reader in front of the guard.
- ◯ A fingerprint reader for logging in to a safety-critical server. Users must use the fingerprint reader attached to the server to log on to the server. The server is in an isolated location and few other people are around.

Question 8: Biometric Templates The following figure shows the distribution of Alice's and Bob's template scores for a new thumbprint reader. Where should Bob's upper threshold be set to minimize the chance of Alice falsely authenticating as Bob?



- ◯ A
- ◯ B
- ◯ C

Question 9: Brute-force Guessing A secret message is encrypted using AES in cipher block chaining mode. An attacker writes a program to launch a known plaintext attack: the attacker knows the first 16 bytes of the ciphertext, the first 16 bytes of the plaintext, and the IV. The attacker also knows `rand()` was used to generate the key. The program, written in C, takes three parameters on the command line: the 16 bytes of plaintext, the 16 bytes of the ciphertext, and the IV. The program launches a brute-force attack, exhaustively trying keys until it finds the key that will produce the given ciphertext for the given plaintext and IV. A snippet of the brute-force attack code is shown in Listing 1.

Listing 1: Brute-force attack code snippet

```
1  # define KEYSIZE 16
2  int main ( int argc , char ** argv )
3  {
4  // initialize and set up buffers
5  ...
6
7    unsigned char key [ KEYSIZE ];
8
9    // ** Describe what is happening here **
10   // Note : UINT_MAX is the largest unsigned int
11   // value , typically 2^32 - 1.
12   for ( int i = 0; i <= UINT_MAX ; i ++ ) {
13     srand ( i );
14     for ( int j = 0; j < KEYSIZE ; j ++){
15       key [ j ] = rand () % 256;
16     }
17
18     // check whether key is the one we want
19     ....
20   }
21 }
```

The attacker runs the program as follows:

```
$ ./brute-force-attack 35100a4624312e35025d0d4c5d35a30a
9938580ddce5f778daf6a75c7e627f65 090807060504030201 00A2B2C2D2E2F2
```

9.1. When the program begins execution (at line 3 in the snippet above), the contents of the first byte of memory pointed to by argv[1] is: (Your answer should be written as a single byte, or 8 bits. Ex: '01010101')

9.2. The value in the byte from part 1 is best understood as:

- ◯ a binary number equal to 3
- ◯ the ASCII encoding of a character digit
- ◯ a packed representation of two digits
- ◯ a decimal constant stored directly in memory

9.3. What is the attacker trying to do in lines 12-16 in Listing 1?