**“Cryptography Essentials” Course Project**

**Instructions:**

*Complete this project and submit it to your instructor. See the assignment page for information about the grading rubric. Do not hesitate to contact your instructor if you have any questions about the project.*

This course project consists of three parts, each of which corresponds to concepts that you will learn throughout the course. Complete each project part as you progress through the course. Wait until all three parts are complete before submitting the project. Begin your course project by completing Part One below.

**Part One: Analyze an Encryption Scheme**

Consider a sample encryption scheme where the key is a random 4-digit pin code denoted by: d1, d2, d3, d4. To encrypt a message m, first break the message up into chunks of four letters. Next, shift each four-letter block of your message by your pin code. For instance, if the key (i.e., the pin code) is 3412, the message GOODMORNING gets encrypted as follows:

**G O O D M O R N I   N G**

3  4 1  2 3  4 1  2 3  4 1

**J  S P F P S  S P L  R H**

Answer the following questions. Please limit your answers to 100 words or less.

|  |  |
| --- | --- |
| Give an informal definition of a private-key encryption scheme. We encourage you to re-watch the videos in this module several times to help you answer this question. | *A private-key encryption scheme answers three questions:*   1. *How do I “get” a key?* 2. *How does a sender use a key to “lock” a message?* 3. *How does a recipient use a key to “unlock” a message?* |
| If the pin code is 7832, what does HELLOWORLD encrypt to? | HELLOWORLD  783278327832  OMONVFRTSL |
| In this sample scheme, how do you decrypt messages given the secret key provided above? |  |
| Is this a good encryption scheme? Why or why not? |  |

**Part Two: Explore the Use of Key Pairs**

Public-key cryptography forms the foundation of secure communications today, so it is important that you solidify your understanding of how key pairs work to encrypt and decrypt messages. Answer the questions below. Please limit your answers to 100 words or less.

|  |  |
| --- | --- |
| Give an informal definition of a public-key encryption scheme and how it differs from a private-key encryption scheme. |  |
| In your own words, explain the difference between a public key and a secret key. |  |
| Think of a business-related data privacy problem or challenge. Describe how you might use public and private keys to solve the problem. |  |
| Think of the communication tools used in your own work environment. Then, list the top two most frequently used tools or applications. Do some research, both internally and on the web, to see what kind of encryption scheme the tools use to protect messages (private-key encryption or public-key encryption). Consider sending a message to someone in your technology department to help you answer the questions to the right. | *Top two tools used for communication:*  *Type of encryption they rely on:*  *Was it easy to find information on the kind of encryption that the tools rely on to secure communications?* |

**Part Three: Devise a Commodity Exchange**

Think of a commodity that could be traded online via a public ledger. For the purposes of this project, you can imagine that this public ledger is equivalent to a public Facebook wall; anyone can see what is posted to the profile. Although it will be missing some key properties to make it secure (i.e. you have to put your trust that Facebook will not tamper with the transactions posted to the public wall), it will be good enough for your fledgling commodity exchange. Below, you will describe how you would use digital signatures to ensure the integrity of the exchange. Please limit your answers to 100 words or less.

|  |  |
| --- | --- |
| Give an informal definition of a digital signature scheme. We recommend that you re-watch the videos in this module several times before attempting to answer this question. In your definition, be sure to include the purposes of a public key and a secret key. |  |
| Describe how you would use the public ledger in combination with digital signatures to create your commodity exchange. Specifically, explain how digital signatures would be used to protect commodities from being stolen. |  |

*To submit this assignment, please refer to the instructions in the course.*