U.S Department of Homeland Security
Washington, DC 20528

Homeland Security

February 22, 2022

MEMORANDUM FOR: Alice Anderson
Field Agent
Central Intelligence Agency

FROM: Carol Clark
Director
U.S. Department of Homeland Security

SUBJECT: **Mission #1 and Key Exchange**

This message is being sent via secure channels to you and to your fellow field agent, Bob Brown. Your first mission is to use **symmetric-key encryption** to send an encrypted message to Bob Brown. In order for this type of encryption to work, both you and Bob must have a shared secret (a password). We have included this shared secret in this memorandum. Please note that this shared secret (password) must be typed exactly in order for Bob to be able to decrypt your message. The shared secret has no spaces, and it is case sensitive:

Shared Secret: *TheDuckFliesAt1237AM*

Please use this shared secret to encrypt the following message and send it to Bob. You must post your encrypted message as text in a Schoology discussion thread.

Secret Message to Send to Bob: *If we successfully complete our mission, we get a treat.*

Unfortunately, our operatives on the ground have determined that an enemy agent, Eve Edwards, will likely be able to intercept all communications between you and Bob. If at any point Eve is able to decrypt one of your messages, you will fail your mission. We have reason to believe that Eve does not know the shared secret in this memo, but it is unknown whether this shared secret will remain secure for future communications.

Note: For this mission, you will be using *http://tinyurl.com/symmetric22*

U.S Department of Homeland Security
Washington, DC 20528

Homeland Security

February 22, 2022

MEMORANDUM FOR: Bob Brown
Field Agent
Central Intelligence Agency

FROM: Carol Clark
Director
U.S. Department of Homeland Security

SUBJECT: **Mission #1 and Key Exchange**

This message is being sent via secure channels to you and to your fellow field agent, Alice Anderson. Your first mission is to use **symmetric-key encryption** to decrypt an encrypted message from Alice Anderson. In order for this type of encryption to work, both you and Alice must have a shared secret (a password). We have included this shared secret in this memorandum. Please note that this shared secret (password) must be typed exactly in order for you to decrypt the message you receive from Alice. The shared secret has no spaces, and it is case sensitive:

Shared Secret: *TheDuckFliesAt1237AM*

You will be receiving your encrypted message as text in a Schoology discussion thread. Unfortunately, our operatives on the ground have determined that an enemy agent, Eve Edwards, will likely be able to intercept all communications between you and Alice. If at any point Eve is able to decrypt any of your messages, you will fail your mission. We have reason to believe that Eve does not know the shared secret in this memo, but it is unknown whether this shared secret will remain secure for future communications.

Note: For this mission, you will be using *http://tinyurl.com/symmetric22*

U.S Department of Homeland Security
Washington, DC 20528

Homeland Security

February 22, 2022

MEMORANDUM FOR: Alice Anderson
Field Agent
Central Intelligence Agency

FROM: Carol Clark
Director
U.S. Department of Homeland Security

SUBJECT: **Mission #2 and Warning of Enemy Operative Activity**

Congratulations on succeeding on your first mission. Unfortunately, we have learned that Eve Edwards now knows your shared secret with Bob. Because of this threat of enemy operative activity, you will no longer be able to use it to encrypt your communications.

Your second mission is to use **asymmetric-key encryption (public-private key encryption)** to send an encrypted message to Bob Brown. In order for this type of encryption to work, you will need to encrypt your secret message using Bob's **public key**.

Please use Bob's **public key** to encrypt the following message and send it to Bob. You must post your encrypted message as text in a Schoology discussion thread.

Secret Message to Send to Bob: *Treat=donuts*

As before, Eve Edwards, will be able to intercept all communications between you and Bob. If at any point Eve is able to decrypt your secret message, you will fail your mission.

Note: For this mission, you will be using *http://tinyurl.com/encrypt22*

U.S Department of Homeland Security
Washington, DC 20528

Homeland Security

February 22, 2022

MEMORANDUM FOR: Bob Brown
Field Agent
Central Intelligence Agency

FROM: Carol Clark
Director
U.S. Department of Homeland Security

SUBJECT: **Mission #2 and Warning of Enemy Operative Activity**

Congratulations on succeeding on your first mission. Unfortunately, we have learned that Eve Edwards now knows your shared secret with Alice. Because of this threat of enemy operative activity, you will no longer be able to use it to encrypt your communications.

Your second mission is to use **asymmetric-key encryption (public-private key encryption)** to decrypt a message from Alice Anderson. In order for this type of encryption to work, you will need to generate a **public/private keypair**.

You must send your **public key** to Alice as text in a Schoology discussion thread. After this, she will send you an encrypted message, which you can decrypt using your **private key**.

As before, Eve Edwards, will be able to intercept all communications between you and Bob. If at any point Eve is able to decrypt your secret message, you will fail your mission.

Note: For this mission, you will be using *http://tinyurl.com/decrypt22*

U.S Department of Homeland Security
Washington, DC 20528

Homeland Security

February 22, 2022

MEMORANDUM FOR: Alice Anderson
Field Agent
Central Intelligence Agency

FROM: Carol Clark
Director
U.S. Department of Homeland Security

SUBJECT: **Mission #3 and Warning of Limited Server Access**

Congratulations on succeeding on your first two missions. For your final mission, you must send a longer message to Bob. Unfortunately for you, you currently have limited server access, so the message is too long for *http://tinyurl.com/encrypt22* to handle on its own. Here is the content of the classified message you must send to Bob:

> **Secret Message to Send to Bob:** *The donuts are in the back of the room under the teacher's desk.*

This time, you must use **asymmetric-key encryption (public/private-key encryption)** and **symmetric-key encryption** in the *right combination* to send your message securely.

Before you start, you may want to sketch out a list of steps describing how you plan to get your message to Bob securely (an **algorithm**).

During this mission, you and Bob may send as many messages back and forth as text files on your Schoology thread as you like. Please remember that all of your communications will be intercepted by Eve. If she is able to decrypt your secret message, then you have failed your mission.

> **Note:** For this mission, you will be using both *http://tinyurl.com/decrypt22* and *http://tinyurl.com/encrypt22*

U.S Department of Homeland Security
Washington, DC 20528

Homeland Security

February 22, 2022

MEMORANDUM FOR: Bob Brown
Field Agent
Central Intelligence Agency

FROM: Carol Clark
Director
U.S. Department of Homeland Security

SUBJECT: **Mission #3 and Warning of Limited Server Access**

Congratulations on succeeding on your first two missions. For your final mission, you must decrypt a longer message from Alice Anderson. Unfortunately for you, you currently have limited server access, so Alice's message is too long for *http://tinyurl.com/encrypt22* to handle on its own.

This time, you must use a combination of **asymmetric-key encryption (public/private-key encryption)** and **symmetric-key encryption** in order to receive/decrypt Alice's message in a secure manner.

Before you start, you may want to sketch out a list of steps describing how you plan to get your message from Alice securely (an **algorithm**).

During this mission, you and Alice may send as many messages back and forth as text on Schoology as you like. But please remember that all of your communications will be intercepted by Eve, and if she is able to decrypt Alice's secret message, then you have failed your mission.

> **Note:** For this mission, you will be using both *http://tinyurl.com/decrypt22* and *http://tinyurl.com/encrypt22*

U.S Department of Homeland Security
Washington, DC 20528

Homeland Security

February 22, 2022

MEMORANDUM FOR: Alice Anderson and Bob Brown
Field Agent
Central Intelligence Agency

FROM: Carol Clark
Director
U.S. Department of Homeland Security

SUBJECT: **Hint #1 for Mission #3**

Our sources have informed us that your review of Encryption Protocol Training Video #1721B was not sufficient to remind you how to securely communicate with each other for Mission #3. Here is a brief overview of what you must do:

1) Use **asymmetric-key encryption (public/private-key encryption)** to exchange a shared secret with each other (also called **key exchange**).
2) Once both parties have a (secure) shared secret, use **symmetric-key encryption** like you did before to share the secret message.

Good luck with completing your mission.

U.S Department of Homeland Security
Washington, DC 20528

Homeland Security

February 22, 2022

MEMORANDUM FOR: Alice Anderson and Bob Brown
Field Agent
Central Intelligence Agency

FROM: Carol Clark
Director
U.S. Department of Homeland Security

SUBJECT: **Hint #2 for Mission #3**

Our sources have informed us that you need more help to complete Mission #3. Here is a more detailed outline of the steps you must follow:

1) **Bob:** Generate a public/private keypair (use *http://tinyurl.com/decrypt22*).
   *Note: Keep your **private** key secure. If Eve were to intercept it, you would fail your mission.*
2) **Bob:** Send the public key to Alice (send as text on Schoology).
   *Note: Eve will intercept this **public** key when you put it onto Schoology, but that's okay as long as you don't accidentally share the **private** key on Schoology.*
3) **Alice:** Pick a short password (symmetric key) that you would like Bob to (eventually) use to decrypt your secret message.
   Note: Keep this password (symmetric key) secure. If Eve were to intercept it, you would fail your mission.
4) **Alice:** Use Bob's public key to encrypt the password (symmetric key) you picked, and send it back to Bob (use *http://tinyurl.com/encrypt22*).
   Note: Eve will intercept this message, but that's okay because she doesn't know Bob's private key.
5) **Bob:** Use your **private** key to decrypt Alice's message (use *tinyurl.com/decrypt22*).
   Note: You and Alice now have a shared secret. This is a shared symmetric key (password).
6) **Alice:** Use your password to encrypt the secret message, and send it to Bob (use *http://tinyurl.com/symmetric22*).
   Note: Eve will intercept this message, but that's okay because she doesn't know your password.
7) **Bob:** Use the shared symmetric key (password) you just discovered to decrypt Alice's message (use *http://tinyurl.com/symmetric22*).

If you made it this far, you have completed your mission. Congratulations!