Practice activity – RSA Encryption/Decryption

In this practice activity, you will apply your knowledge of public key cryptography to securely transmit a sensitive piece of information from your company to a business partner. You will first generate a private/public key. You will then encrypt some text using the public key of your business partner and subsequently decrypt it (acting as the business partner) using the private key.

RSA (Rivest–Shamir–Adleman) is one of the most popular asymmetric (public key) cryptographic algorithms. RSA supports several different key sizes including 1024, 2048 and 4096 bits.

Resources:

- **Text to Encrypt**: "*This is a confidential sentence that needs to be encrypted*"
- **Public Key Cryptography Algorithm to be used**: RSA
- **Key length**: 1024 bits
- **RSA Key Generator and Encrypt/Decrypt:**

  Online: *https://www.javainuse.com/rsagenerator*

Step 1

Please generate a 1024-bit private/public key pair based on RSA and save both the private and public keys. Please note that this step would normally be performed by your business partner, and they will only share their public key with your company.

Step 2

Please encrypt the text "*This is a confidential sentence that needs to be encrypted*" using the public key of your business partner and save the generated ciphertext.

Step 3

Acting as the business partner, please decrypt the ciphertext that you generated in Step 2 using the private key and verify if the message contents match the original text.

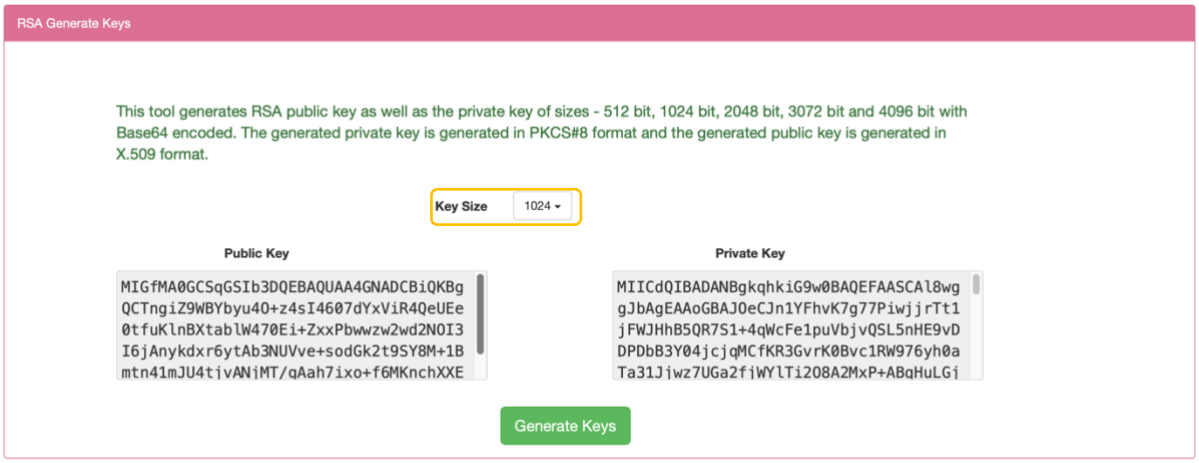
Solution on next page.

Solution

Step 1

Acting as the business partner, we first generate a 1024-bit private/public key pair.

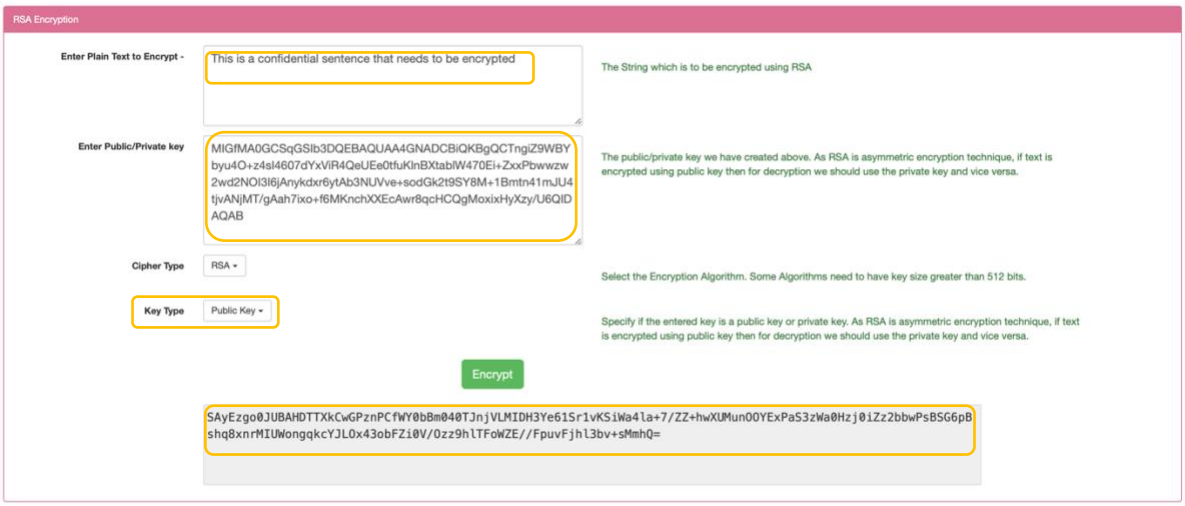
Online: *https://www.javainuse.com/rsagenerator*



Step 2

We provide the plaintext and use the public key to encrypt it.

Online: *https://www.javainuse.com/rsagenerator*

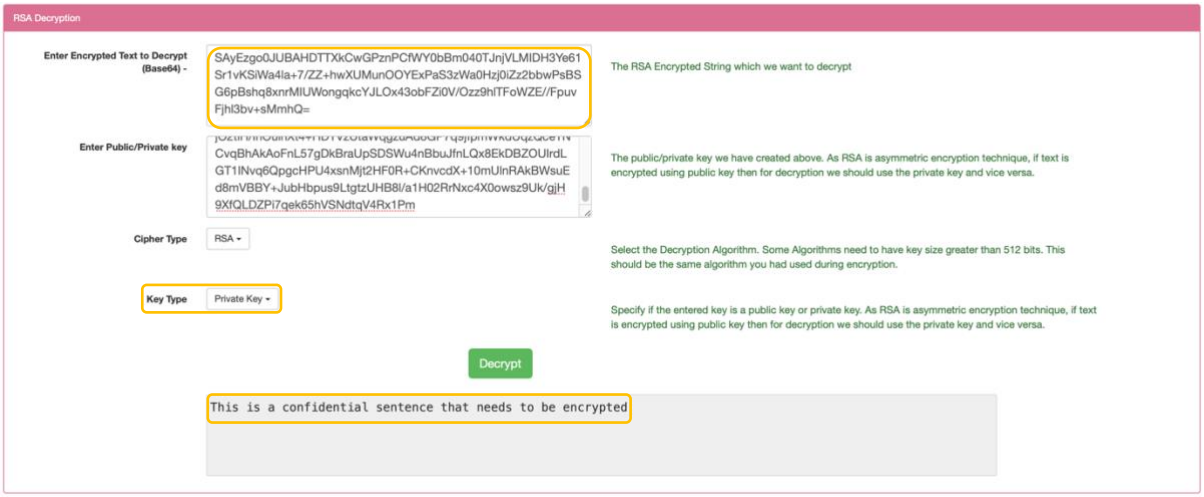


Please note this in this case, we are using the **public key** of our business partner to encrypt so that no one else can decrypt it except for our business partner who has the **private key**. As discussed in the lecture, the public key **cannot** be used again to decrypt the message which was encrypted with the public key.

Step 3

Assuming we are the business partner, we provide the ciphertext and use the private key to decrypt it.

Online: *https://www.javainuse.com/rsagenerator*



As a practice activity, you can try decrypting the ciphertext using the public key, but you will see that it will not give us the correct output and will display error, thus ensuring the confidentiality of the message and providing assurance that only the destination with the private key can decrypt the message.

Congratulations! You have successfully generated RSA key pairs as well as seen public key cryptography in action.