RSA Encryption

What is RSA?

- Asymmetric encryption
  - Uses private and public keys

Terms:

Public key: A key that anyone has access to

Private key: A key that only the owner has access to

Public key can be used to encrypt

Private key is the only key that can decrypt

How are keys generated?

Terms:

- Key: a piece of information that is used to transform data
- Prime numbers: numbers that can’t be divided by anything other than 1 and itself

Keys are generated:

- Multiplying two very large prime numbers together
- Example: 7*19 = 133
- Very hard to guess the two numbers(i.e. 7 and 19) that make the product(133) so it is very hard to guess the key

Encryption process

What do you need?

- Data to encrypt
- Intended public key

Procedure:

- RSA encrypts the data using the public key and math operations
  - Turns plaintext into a numerical value “m”
  - N = product of two prime numbers
  - Ciphertext = m^e mod(n)
  - E = random number

Decryption process

Procedure:

- Turn ciphertext back to plaintext
- How? Reverse the equation
- m = c^d mod n

Variables:

M = original message

C = ciphertext

D = private key component

N = modulus

Applications of RSA Encryption

Why is it important?

- Online messaging
- Secure messaging
- Data protection

Example!

Use google to encrypt the following plaintext:

1. Hello
2. Encryption
3. Calculate

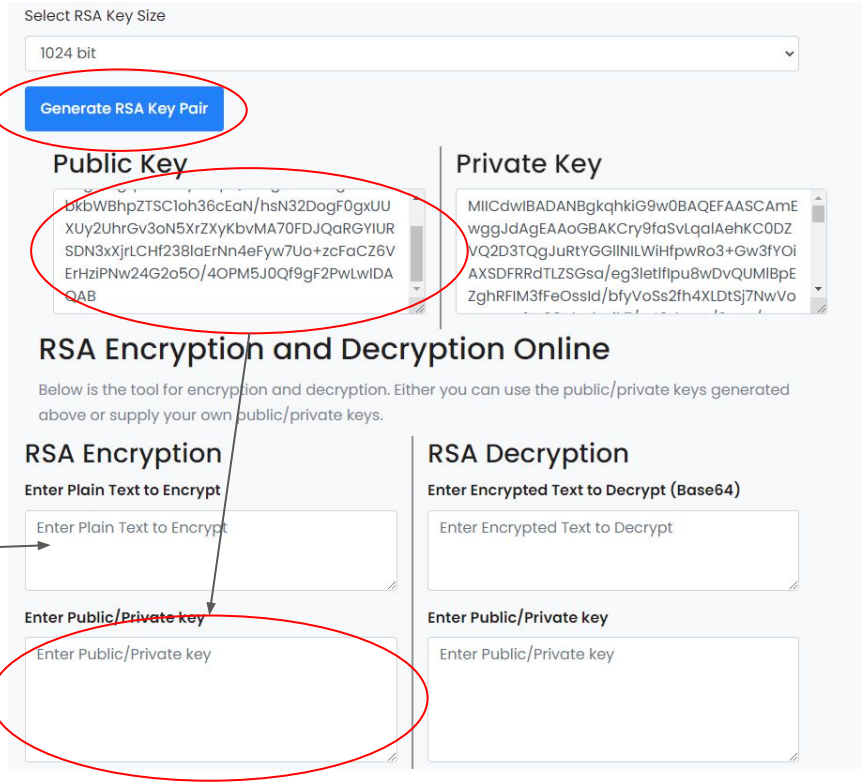
Use website: https://www.devglan.com/online-tools/rsa-encryption-decryption

Instructions Part 1:

1. Press “Generate RSA Key Pair” button
2. Enter plaintext into the box
3. Copy and paste **public key** data into the “public key”
4. Change “select cipher type” to RSA

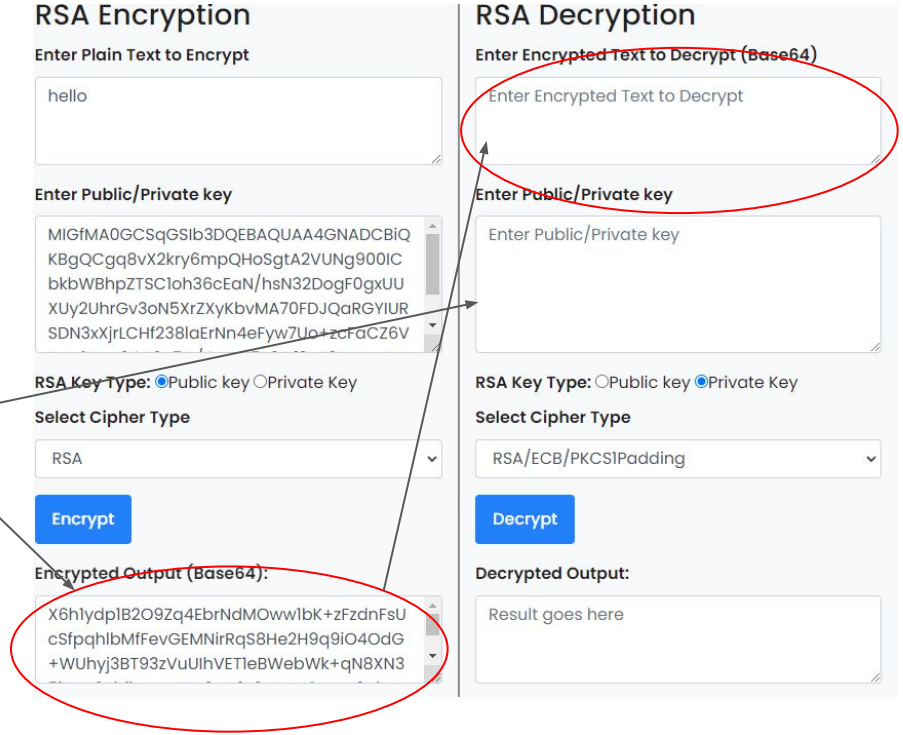
Plaintext:

1. Hello
2. Encryption
3. Calculate



Instructions Part 2:

1. Scroll down to find encrypted text(ciphertext)
2. Copy and paste ciphertext to encrypted text in the RSA decryption column
3. Put the **private key** into the “Enter public/private key” box
4. Change “select cipher type” to RSA



Supplementary Resources(skip if no more time)

1. The math behind RSA encryption:
    a. Use math equation to encrypt “hello”
        i. p = 3, q = 11, and e = 7
        ii. N = p*q
2. Convert “hello” to ASCII values:
    a. H: 72
    b. E: 69
    c. L: 76
    d. L: 76
    e. O: 79

Supplementary P2

3. Use equation: c = m^e mod n

What (mod n) does is it divides (m^e) by “n” and gets the remainder

4. Implement equation(answer in speaker notes):

a. H: 72
b. E: 69
c. L: 76
d. L: 76
e. O: 79

Info:

- M = the digit corresponding to the letter
- E = 7
- N = 33

What is the ciphertext?

Conclusion:

Is the decrypted text the same as the original text?

Final reminders:

- RSA is used to encrypt data
- By encrypting data, RSA is able to protect data from people who shouldn’t be able to access it
- RSA is an asymmetric encryption method
    - This means there is a public and private key

THANKS FOR LISTENING