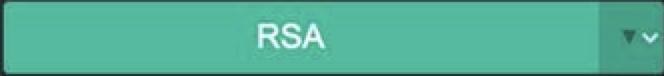
**Welcome to Cryptography Interactive Learning System!**

**I want to learn: **

**Why RSA?**

**(Click it will show introduction and intention)**

Let’s start with **encryption:**

(Click encryption will show the following)

**Method ⋁**

(hide steps before click on them, just like Chegg solutions)

|  |
| --- |
| **Step 1 of 3 ⋁** |
| **Step 2 of 3 ⋁** |
| **Step 3 of 3 ⋁** |

**Example ⋁** (Hide example before user click on example)

|  |
| --- |
| **Step 1 of 3 ⋁** |
| **Step 2 of 3 ⋁** |
| **Step 3 of 3 ⋁** |

**Are you ready to try it yourself? Yes**

(Hide the following until user click  **Yes** )

**Click here to see how to how to choose your numbers**

**(Click here: new tab to prime generator website)**

**or click on dice to generate a random prime number for you**

**prime p: input a prime number here 🎲**

**prime q: input a prime number here 🎲**

**exponent e: input an exponent here 🎲**

**Click Check to see if your number work**

**(Check -> backend, 1. check if p, q is prime, 2. check if e works for inputted p and q**

**And show up the following)**

**N : hint: N = p x q Check if it’s correct**

**(if it’s correct -> show correct under the button, vice versa)**

**r : hint: r = (p-1) x (q-1) Check if it’s correct**

**(if it’s correct -> show correct under the button, vice versa)**

**c : hint: c ≡ me (mod N) Check if it’s correct**

**(if it’s correct -> show correct under the button, vice versa)**

**(show the following after click Check for c)**

**GREAT JOB! You have finished encryption!**

**Your encrypted message is:**

**… …**

**Now, let’s do decryption!**

**d : hint: de ≡ 1 (mod (p − 1)(q − 1)) Check if it’s correct**

**(if it’s correct -> show correct under the button, vice versa)**

**m’: m’ = cd (mod N) . Check if it’s correct**

**(if it’s correct -> show correct under the button, vice versa)**

**You will find out m’ is the same as your inputted message m!**