Jacob S. Santos 09/09/24

BSCOE 4-1 Dr. Ariel Sison

Assignment

P	Base	A	B
23	29	13	19

A:

Step 1: Computer A selects a random secret whole number

$$R = 13$$

Step 2: Computer A raises the base number to the power of the secret number

$$B^R = 29^{13} = 10260628712958602189$$

Step 3: Computer A divides the result of the calculation by the prime number selected.

$$\frac{10260628712958602189}{23} = 446114291867765312.5652173913043478$$

Step 4: To get the remainder multiply the whole number of the quotient to the prime number then subtract it from the dividend

$$remainder = 446114291867765312 \times 23 = 10260628712958602176$$

$$10260628712958602189 - 10260628712958602176 = 13$$

Computer A sends **remainder 13** to Computer B

B:

Step 1: Computer B selects a random secret whole number

$$R = 19$$

Step 2: Computer B raises the base number to the power of the secret number

$$B^R = 29^{19} = 6103261246589991489578849669$$

Step 3: Computer A divides the result of the calculation by the prime number selected.

$$\frac{6103261246589991489578849669}{23} = 265359184634347456068645637.7826086956521739$$

Step 4: To get the remainder multiply the whole number of the quotient to the prime number then subtract it from the dividend

$$remainder = 265359184634347456068645637 \times 23 = 6103261246589991489578849651$$

$$6103261246589991489578849669 - 6103261246589991489578849651 = 18$$

Computer B sends **remainder 18** to Computer A

Then,

Computer A raises the **remainder 18** to the power of its randomly selected number then divides resulting number by the prime number that they had selected earlier

$$18^{13} = 20822964865671168$$

$$\frac{20822964865671168}{23} = 905346298507442.0869565217391304$$

To get the remainder multiply the whole number of the quotient to the prime number then subtract it from the dividend

$$remainder = 905346298507442 \times 23 = 20822964865671166$$

$$20822964865671168 - 20822964865671166 = \mathbf{2}$$

Computer B raises the remainder that it got from Computer A (**which is 13**) to the power of its randomly selected number 19

$$13^{19} = 1461920290375446110677$$

$$\frac{1461920290375446110677}{23} = 63561751755454178725.0869565217391304$$

To get the remainder multiply the whole number of the quotient to the prime number then subtract it from the dividend

$$remainder = 63561751755454178725 \times 23 = 1461920290375446110675$$

$$1461920290375446110677 - 1461920290375446110675 = \mathbf{2}$$

As we can see both the remainders of A and B is 2, the secret key in this case is 2.