

Started on	Thursday, 8 December 2022, 5:04 AM
State	Finished
Completed on	Thursday, 8 December 2022, 5:18 AM
Time taken	13 mins 46 secs
Grade	1.50 out of 1.50 (100%)

Question **1**

Correct

Mark 0.75 out of 0.75

- Consider the RSA cryptosystem with the following setting:
- Use a 27-letter alphabet for plaintext and ciphertext:
_ (notation for blank) with numerical equivalent 0 and letters A-Z (the English alphabet) with numerical equivalents 1-26.
 - Plaintext message units are blocks of $k = 2$ letters, whereas ciphertext message units are blocks of $l = 3$ letters.
 - The modulus $n = pq$, where $p = 31$ and $q = 71$.
 - You must choose the encryption exponent e as the smallest valid odd prime (pay attention to the required condition!).

Encrypt the plaintext DUBLIN.

Solution.

Values:

$n =$ ✓ $\varphi(n) =$ ✓ $e =$ ✓

Plaintext:

Blocks of k letters: ✓ ✓ ✓

Numerical equivalents: $b_1 =$ ✓ $b_2 =$ ✓ $b_3 =$ ✓

Encryption:

$c_1 = b_1^e \bmod n =$ ✓ $c_2 = b_2^e \bmod n =$ ✓ $c_3 = b_3^e \bmod n =$ ✓

Blocks of l letters: ✓ ✓ ✓

Ciphertext: ✓

Question **2**

Correct

Mark 0.75 out of 0.75

- Consider the RSA cryptosystem with the following setting:
- Use a 27-letter alphabet for plaintext and ciphertext:
_ (notation for blank) with numerical equivalent 0 and letters A-Z (the English alphabet) with numerical equivalents 1-26.
 - Plaintext message units are blocks of $k = 2$ letters, whereas ciphertext message units are blocks of $l = 3$ letters.
 - The modulus $n = pq$, where $p = 31$ and $q = 59$.
 - You must choose the encryption exponent e as the smallest valid odd prime (pay attention to the required condition!).
 - The decryption exponent d is determined by e and must be filled in as a positive number mod $\varphi(n)$.

Decrypt the ciphertext _CI_SW_IX.

Solution.

Values:

$n =$ ✓ $\varphi(n) =$ ✓ $e =$ ✓ $d =$ ✓

Ciphertext:

Blocks of l letters: ✓ ✓ ✓

Numerical equivalents: $c_1 =$ ✓ $c_2 =$ ✓ $c_3 =$ ✓

Decryption:

$b_1 = c_1^d \bmod n =$ ✓ $b_2 = c_2^d \bmod n =$ ✓ $b_3 = c_3^d \bmod n =$ ✓

Blocks of k letters: ✓ ✓ ✓

Plaintext: ✓