Question **1**

Correct

Mark 0.50 out of 0.50

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 $p = 37$ and $q = 79$.**
- **You must choose the encryption exponent e as the smallest valid odd prime (pay attention to the required condition!).**

Encrypt the plaintext VIENNA.

Solution.

Values:

n= 2923 ☐ $\varphi(n)$= 2808 ☐ e= 5 ☐

Plaintext:

Blocks of k letters: VI ☐ EN ☐ NA ☐

Numerical equivalents: b_1= 603 ☐ b_2= 149 ☐ b_3= 379 ☐

Encryption:

$c_1 = b_1^e \bmod n$= 1359 ☐ $c_2 = b_2^e \bmod n$= 2887 ☐ $c_3 = b_3^e \bmod n$= 1255 ☐

Blocks of l letters: AWI ☐ CYY ☐ ASM ☐

Ciphertext: AWICYYASM ☐

Question **2**

Correct

Mark 0.50 out of 0.50

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 $p = 61$ and $q = 71$.**
- **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 CLPAYQCMJ.

Solution.

Values:

n= 4331 ☐ $\varphi(n)$= 4200 ☐ e= 11 ☐ d= 2291 ☐

Ciphertext:

Blocks of l letters: CLP ☐ AYQ ☐ CMJ ☐

Numerical equivalents: c_1= 2527 ☐ c_2= 1421 ☐ c_3= 2548 ☐

Decryption:

$b_1 = c_1^d \bmod n$= 59 ☐ $b_2 = c_2^d \bmod n$= 498 ☐ $b_3 = c_3^d \bmod n$= 257 ☐

Blocks of k letters: BE ☐ RL ☐ IN ☐

Plaintext: BERLIN ☐