Home / My courses / PKC / Assignment C (Week 8) - max. 1.5 points / Assignment C (to submit by Week 10)

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** Consider the RSA cryptosystem with the following setting: Correct • Use a 27-letter alphabet for plaintext and ciphertext: Mark 0.75 out of $_$ (notation for blank) with numerical equivalent 0 and letters A-Z (the English alphabet) with numerical equivalents 1-26. 0.75 • 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: $\varphi(n)=$ 2100 n = |2201|**Plaintext:** Blocks of *k* letters: DU Numerical equivalents: $b_1 = 129$

 $c_3 = b_3^e \bmod n = 2122$

Question **2**Correct

Mark 0.75 out of 0.75

 $\label{lem:consider} \textbf{Consider the RSA cryptosystem with the following setting:}$

- ullet 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.

BXP

- 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 $\varphi(n)$.

 $c_2 = b_2^e \mod n$ = 66

Decrypt the ciphertext _CI_SW_IX.

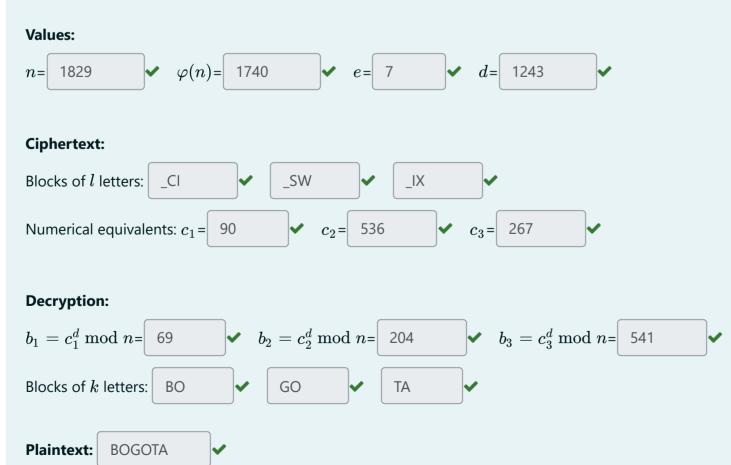


Encryption:

 $c_1 = b_1^e \mod n = 521$

Blocks of *l* letters: _SH

Ciphertext: _SH_BLBXP



■ Assignment B (to submit by Week 10)

Jump to... \$

Assignment C (to submit by Week 12) ►