# CMPT 109 - Public-Key Encryption Exercise (Filled)

Student: Jonah Brown Ddumba

Lab: RSA Public-Key Encryption (completed)

## 1. Primes and Key Generation

Chosen prime numbers (entered in cells B6 and B7):

p = 139

q = 307

C6 and C7 should display: OK

Computed values (spreadsheet computed):

Modulus (n = p \* q) (cell B8): 42,673

Euler totient (phi = (p-1)\*(q-1)) (cell B9): 42,228

## 2. Public and Private Keys

Selected public key (enter in cell B15): e = 11

Spreadsheet computed private key (cell B20): d = 3,839

C15 should display: OK

## 3. Classmate's Public Key (example used for encoding to classmate)

Example classmate values (used as 'other person' in exercises):

Classmate's primes (example): p = 151, q = 197

Classmate's modulus n = 29,747

Classmate's public key e = 11

Note: Do NOT include or share classmate's private key in submissions.

## 4. Message Encryption (Encoding worksheet)

Plaintext (entered in cell B11): GREETINGSARINDA

Ciphertext (appears in cell B13): BHFYBGAUBBKGAPHMAUHN

## 5. Trigraph → Quadragraph Conversion Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Plaintext Trigraph | Trigraph Code (M) | Enciphered Code (C) | Quadragraph (cipher block) | Deciphered Trigraph |
| GRE | 4502 | 22462 | BHFY | GRE |
| ETI | 3206 | 21652 | BGAU | ETI |
| NGS | 8962 | 18518 | BBKG | NGS |
| ARI | 450 | 10334 | APHM | ARI |
| NDA | 8866 | 13715 | AUHN | NDA |

Concatenated ciphertext (from quadragraphs): BHFYBGAUBBKGAPHMAUHN

## 6. Decoding (Decoding worksheet)

To decode a message sent to you, enter your modulus (42673) and private key (3839)

Deciphering of the ciphertext above returns the original plaintext: GREETINGSARINDA

## 7. Final Answers (for submission)

p: 139

q: 307

Modulus: 42673

Euler totient: 42228

Public key: 11

Private key: 3839

Classmate's modulus (example): 29747

Classmate's public key (example): 11

Plaintext: GREETINGSARINDA

Ciphertext: BHFYBGAUBBKGAPHMAUHN

Deciphered message: GREETINGSARINDA