

## Question 1

Encoding *LETSSAILFORTHESPANISHMAIN* with key *PIECESOFEIGHT* gave

AMXUWSWQJWXAATATCRAGMQIOU

## Question 2

Decoding *ZVTVKGVBLNWYJVCLBOOHSSKFIGWYOEDNZ* with key *GOLDCOINS* gave

THISISNOTHINGTODOWITHPIRATESATALL

## Question 3

Using  $C1$ ,  $C2$ , and  $C3$ , the following  $M$  was found

ASSOONASWESTARTEDPROGRAMMINGWEFOUNDTOOOURSURPRISETHATITWASNT  
ASEASYTOGETPROGRAMSRIGHTASWEHADTHOUGHTDEBUGGINGHADTOBE  
DISCOVEREDICANREMEMBERTHEEXACTINSTANTWHENIREALIZEDTHATALARGE  
PARTOFMYLIFEFROMTHENONWASGOINGTOBESPENTINFINDINGMISTAKESINMY  
OWNPROGRAMSMAURICEWILKESDISCOVERSDDEBUGGING

Please note, line breaks were added for readability, and are **not** part of the original message

## Question 4

Calculations done by code, showing intermediate steps exactly as output from RSA.py

$$17^{54} \bmod 139 = 125$$

$$17^1 = 17 \bmod 139$$

$$17^2 = 11 \bmod 139$$

$$17^4 = 121 \bmod 139$$

$$17^8 = 46 \bmod 139$$

$$17^{16} = 31 \bmod 139$$

$$17^{32} = 127 \bmod 139$$

Starting with  $17^{32} \bmod 139$

Multiplying by  $17^{16}$ , to reach  $17^{48} \bmod 139$

Multiplying by  $17^4$ , to reach  $17^{52} \bmod 139$

Multiplying by  $17^2$ , to reach  $17^{54} \bmod 139$

Calculated  $17^{54} \bmod 139 = 125$

$$2345^{65531} \bmod 265189 = \mathbf{32548}$$

$$2345^1 = 2345 \bmod 265189$$

$$2345^2 = 195245 \bmod 265189$$

$$2345^4 = 221653 \bmod 265189$$

$$2345^8 = 77513 \bmod 265189$$

$$2345^{16} = 143185 \bmod 265189$$

$$2345^{32} = 182635 \bmod 265189$$

$$2345^{64} = 70805 \bmod 265189$$

$$2345^{128} = 215169 \bmod 265189$$

$$2345^{256} = 207374 \bmod 265189$$

$$2345^{512} = 132069 \bmod 265189$$

$$2345^{1024} = 209853 \bmod 265189$$

$$2345^{2048} = 200702 \bmod 265189$$

$$2345^{4096} = 144460 \bmod 265189$$

$$2345^{8192} = 173623 \bmod 265189$$

$$2345^{16384} = 116932 \bmod 265189$$

$$2345^{32768} = 212973 \bmod 265189$$

Starting with  $2345^{32768} \bmod 265189$

Multiplying by  $2345^{16384}$ , to reach  $2345^{49152} \bmod 265189$

Multiplying by  $2345^{8192}$ , to reach  $2345^{57344} \bmod 265189$

Multiplying by  $2345^{4096}$ , to reach  $2345^{61440} \bmod 265189$

Multiplying by  $2345^{2048}$ , to reach  $2345^{63488} \bmod 265189$

Multiplying by  $2345^{1024}$ , to reach  $2345^{64512} \bmod 265189$

Multiplying by  $2345^{512}$ , to reach  $2345^{65024} \bmod 265189$

Multiplying by  $2345^{256}$ , to reach  $2345^{65280} \bmod 265189$

Multiplying by  $2345^{128}$ , to reach  $2345^{65408} \bmod 265189$

Multiplying by  $2345^{64}$ , to reach  $2345^{65472} \bmod 265189$

Multiplying by  $2345^{32}$ , to reach  $2345^{65504} \bmod 265189$

Multiplying by  $2345^{16}$ , to reach  $2345^{65520} \bmod 265189$

Multiplying by  $2345^8$ , to reach  $2345^{65528} \bmod 265189$

Multiplying by  $2345^2$ , to reach  $2345^{65530} \bmod 265189$

Multiplying by  $2345^1$ , to reach  $2345^{65531} \bmod 265189$

Calculated  $2345^{65531} \bmod 265189 = 32548$

$$4733459^{65537} \bmod 75968647 = \mathbf{621879}$$

$$4733459^1 = 4733459 \bmod 75968647$$

$$4733459^2 = 49107677 \bmod 75968647$$

$$4733459^4 = 16238929 \bmod 75968647$$

$$4733459^8 = 67757406 \bmod 75968647$$

$$4733459^{16} = 25488171 \bmod 75968647$$

$$4733459^{32} = 64480977 \bmod 75968647$$

$$4733459^{64} = 57889554 \bmod 75968647$$

$$4733459^{128} = 19358089 \bmod 75968647$$

$$4733459^{256} = 50744319 \bmod 75968647$$

$$4733459^{512} = 56497489 \bmod 75968647$$

$$4733459^{1024} = 54825938 \bmod 75968647$$

$$4733459^{2048} = 38930457 \bmod 75968647$$

$$4733459^{4096} = 49024383 \bmod 75968647$$

$$4733459^{8192} = 51007254 \bmod 75968647$$

$$4733459^{16384} = 24313 \bmod 75968647$$

$$4733459^{32768} = 59341440 \bmod 75968647$$

$$4733459^{65536} = 51988154 \bmod 75968647$$

Starting with  $4733459^{65536} \bmod 75968647$

Multiplying by  $4733459^1$ , to reach  $4733459^{65537} \bmod 75968647$

Calculated  $4733459^{65537} \bmod 75968647 = 621879$

**Question 5 - You wish to securely send the message  $M=654733$  to the bank**

**i) State the calculation to encrypt this message for sending to the bank**

$$C = M^{e_{bank}} \bmod n_{bank}$$

$$C = 654733^{65537} \bmod 76282747$$

**ii) State the encrypted value, calculated using your code**

39964485

### Question 6 - The bank sends you an encrypted message 1684446

i) State the calculation used in decryption

$$C^{d_{mine}} = M^{e_{mine} d_{mine}} = M \bmod n_{mine}$$

$$C^{3497603} = M^{1676267 \cdot 3497603} = M \bmod 9436709$$

ii) What is the decrypted value in this case?

1101011

### Question 7 - The bank requests a signed encrypted message from you so that they can verify that you are the sender and the message is secure in transmission to them.

You should encrypt the message and signature as two separate blocks. They already know your public key.

i) State the calculation to sign and encrypt the message 337722

TODO

ii) What is the transmission made for the message 337722 when it has been signed and encrypted?

TODO