Task: Encrypt / Decrypt the 4 letters of my surname with RSA

Stage 1: key generation

We pick two random primes:

$p = 47$, $q = 29$

Let $n = 47 \cdot 29 = 1363$ be their product

And $\varphi(n) = (p-1)(q-1) = 46 \cdot 28 = 1288$

Select a random number e st $1 < e < \varphi(n)$

let $e = 13$; $\gcd(1288, 13) = 1$ true

So we have the public key $\underline{k_E = (1363, 13)}$

We compute the private key d:

$d = e^{-1} \bmod \varphi(n)$

$= 13^{-1} \bmod 1288$

We use the extended Euclidean algorithm

$1288 = \underline{13} \cdot 99 + \underline{1}$

By Bezout's identity we know that $ax + by = \gcd(a, b)$

$\Rightarrow 1288 \cdot 1 + 13 \cdot (-99) = 1$

$\Rightarrow \underline{d = -99}$, private key

Stage 2 : Encryption

public key: $(n, e) = (1363, 13)$; $k = 2$; $l = 3$

private key: $d = -99$

message = RA RE

(this is actually 486, I misswrote)

(Here I did the mistake I mention at the end)

$RA = 18 \cdot 27 + 1 = 487 + 1 = 488$

$RE = 18 \cdot 27 + 5 = 487 + 5 = 492$

We encrypt each chunk using the formula: $m^e \bmod n$

1°. $488^{13} \bmod 1363 =$

We compute this using the repeated squaring modular expo.

$13 = 2^0 \cdot 2^2 + 2^3$

$488^{(2^0)} = \underline{488}$

$488^{(2^1)} = (488^{(2^0)} \cdot 488^{(2^0)}) \bmod 1363 = 982$

$488^{(2^2)} = (488^{(2^1)} \cdot (488)^{(2^1)}) \bmod 1363 = \underline{683}$

$488^{(2^3)} = 488^{(2^2)} \cdot 488^{(2^2)} \bmod 1363 = \underline{343}$

$\rightarrow 488^{13} \bmod 1363 = (488 \cdot 683 \cdot 343) \bmod 1363 = \boxed{284}$

2°. $492^{13} \bmod 1363 =$

$492^{(2^0)} = \underline{492}$

$492^{(2^1)} = (492^{(2^0)} \cdot 492^{(2^0)}) \bmod 1363 = 813$

$492^{(2^2)} = (492^{(2^1)} \cdot 492^{(2^1)}) \bmod 1363 = \underline{1277}$

$492^{(2^3)} = (492^{(2^2)} \cdot 492^{(2^2)}) \bmod 1363 = \underline{581}$

$\rightarrow 492^{13} \bmod 1363 = (492 \cdot 581 \cdot 1277) \bmod 1363 = \boxed{1159}$

So the encrypted chunks have numerical rep:

$$RA \xrightarrow{\text{encrypted}} 284$$
$$RE \xrightarrow{\text{encrypted}} 1159$$

And to get their literal equivalents we write them in base 27.

$$284 = \boxed{0} \cdot 27^2 + \boxed{10} \cdot 27^1 + \boxed{14} \cdot 27^0 \Rightarrow \_JN$$
$$1159 = \boxed{1} \cdot 27^2 + \boxed{15} \cdot 27^1 + \boxed{25} \cdot 27^0 \Rightarrow AOY$$

<u>Stage 3</u>: Decryption

We use the private key $d = -99$ and the formula

$$m = c^d \bmod n$$
$$= c^{-99} \bmod 1363$$

I do not know how to compute the modulo of a number with negative exponent, BUT, using Euler's totient theorem and some help from the internet (links included in email) we can do a little trick.

From Euler's totient theorem we have

$$a^{\varphi(n)} \equiv 1 \bmod n \quad \text{if } n \text{ and } a \text{ are coprime}$$

So in my case I have:

$$\gcd(284, 1363) = 1$$
$$\text{So, } 284^{\varphi(1363)} = 1 \bmod 1363$$
$$\Rightarrow 284^{1288} = 1 \bmod 1363$$

Since this result is 1 under modulo 1363, we can multiply with 284^{-99} and it will yield the same result.

After which we use the repeated squaring mod. exp

$\Rightarrow 284^{-99} \cdot 284^{\varphi(n)} = 284^{-99} \cdot 284^{1288} = 284^{1189}$

(*) The same thing applies to 1159, because gcd(1159, 1363)=1)

$284^{1189} \bmod 1363 =$

$1189 = 2^{10} + 2^{7} + 2^{5} + 2^{2} + 2^{0}$

$284^{(2^0)} = 284$

$284^{(2^1)} = (284^{(2^0)} \cdot 284^{(2^0)}) \bmod 1363 = 239$

$284^{(2^2)} = (284^{(2^1)} \cdot 284^{(2^1)}) \bmod 1363 = 1238$

$284^{(2^3)} = (284^{(2^2)} \cdot 284^{(2^2)}) \bmod 1363 = 632$

$284^{(2^4)} = (284^{(2^3)} \cdot 284^{(2^3)}) \bmod 1363 = 65$

$284^{(2^5)} = (284^{(2^4)} \cdot 284^{(2^4)}) \bmod 1363 = 136$

$284^{(2^6)} = (284^{(2^5)} \cdot 284^{(2^5)}) \bmod 1363 = 777$

$284^{(2^7)} = (284^{(2^6)} \cdot 284^{(2^6)}) \bmod 1363 = 1283$

$284^{(2^8)} = (1283 \cdot 1283) \bmod 1363 = 984$

$284^{(2^9)} = (984 \cdot 984) \bmod 1363 = 487$

$284^{(2^{10})} = (284^{(2^9)} \cdot 284^{(2^9)}) \bmod 1363 = 7$

$284^{1189} \bmod 1363 = (284 \cdot 1238 \cdot 136 \cdot 1283 \cdot 7) \bmod 1363 = \boxed{488}$

$1159^{1189} \mod 1363$

$1189 = 2^{10} + 2^{7} + 2^{5} + 2^{2} + 2^{0}$

$1159^{(2^0)} = \underline{1159}$

$1159^{(2^1)} = 1159^{(2^0)} \cdot 1159^{(2^0)} \mod 1363 = 726$

$1159^{(2^2)} = 1159^{(2^1)} \cdot 1159^{(2^1)} \mod 1363 = \underline{958}$

$1159^{(2^3)} = 1159^{(2^2)} \cdot 1159^{(2^2)} \mod 1363 = 465$

$1159^{(2^4)} = 1159^{(2^3)} \cdot 1159^{(2^3)} \mod 1363 = 871$

$1159^{(2^5)} = 1159^{(2^4)} \cdot 1159^{(2^4)} \mod 1363 = \underline{813}$

$1159^{(2^6)} = 1159^{(2^5)} \cdot 1159^{(2^5)} \mod 1363 = 1277$

$1159^{(2^7)} = 1159^{(2^6)} \cdot 1159^{(2^6)} \mod 1363 = \underline{581}$

$1159^{(2^8)} = 1159^{(2^7)} \cdot 1159^{(2^7)} \mod 1363 = 900$

$1159^{(2^9)} = 1159^{(2^8)} \cdot 1159^{(2^8)} \mod 1363 = 378$

$1159^{(2^{10})} = 1159^{(2^9)} \cdot 1159^{(2^9)} \mod 1363 = \underline{1132}$

$1159^{1189} \mod 1363 = (1132 \cdot 581 \cdot 813 \cdot 958 \cdot 1159) \mod 1363$

$= \boxed{492}$

So our decrypted numbers are

488 , 492

We write them in base 27 to get their literal equivalents:

$488 = 18 \cdot 27 + 2 \Rightarrow RB$

$492 = 18 \cdot 27 + 5 \Rightarrow RF$

I miss calculated when I wrote RARE at the begging of the exercise, but the encryption/decryption appears correct. I encrypted RBRF by mistake.