Examples

Example 1 Take $p = 11$ and $q = 13$ to be our two primes p, q. So $n = 143$ and $\phi(n) = (11-1)(13-1) = 120$.

We choose an integer a relatively prime to $\phi(n) = 120$: Say $a = 41$. Express 1 as a linear combination of 120 and 41:

$$41 \cdot 41 - 14 \cdot 120 = 1$$

so 'x' is 41. We publish $(n,a) = (143,41)$.

To encode a block β, the sender calculates $\beta^{41} \mod 143$, and to decode a received block m, we calculate $m^{41} \mod 143$.

Thus, for example, to encode the message $\beta = 65$, the sender computes

$$65^{41} \mod 143 = 65 \mod 143$$

and so sends $m = 65$. On receipt of this message, anyone who knows 'x' (the inverse of $41 \mod 143$) computes $65^{41} \mod 143$ which is equal to the original message 65.

If now we use the number-to-letter equivalents:

G = 1, O = 2, L = 3, D = 4,

and the received message is $12/46$, the original message is decoded by calculating

$$12^{41} \equiv 12 \mod 143$$

and

$$46^{41} \equiv 24 \mod 143$$

Juxtaposing these blocks gives 1224, and so the message was the word G O O D.

(In this example we used small primes for purposes of illustration but, in doing so, violated the requirement that the number of digits in any block should be less than the number of digits in either of the primes chosen.)

Example 2 Take $p = 1000000000100011$ and $q = 2222222222222222221$ to be our two primes p, q. So $n = 2222222222244444688766666666665544431$ and

$$\phi(n) = (1000000000100011 - 1)(2222222222222222221 - 1) = 2222222222244444666444444444444222200$$

We choose an integer a relatively prime to $\phi(n)$: Say $a = 1394948628539116065243497744947323$. Express 1 as a linear combination of $\phi(n)$ and a:

$$1197259832153669065418818764965 87 \cdot a - 7515521823153171047527268427710 3 \cdot \phi(n) = 1$$

so 'x' is 119725983215366906541881876496587. We publish

$$(n,a) = (2222222222244444688766666666665544431, 1394948628539116065243497744947323)$$

To encode a block β, the sender calculates $\beta^{a} \mod n$, and to decode a received block m, we calculate $m^{x} \mod n$.

Thus, for example, to encode the message $\beta = 22$, the sender computes

$$\begin{aligned} &22^{1394948628539116065243497744947323} \\ &\equiv 16364470376360086663129822523842 2 \mod 2222222222244444688766666666665544431 \end{aligned}$$

and so sends $m = 163644703763600866631298225238422$. On receipt of this message, anyone who knows 'x' (the inverse of $a \mod n$) computes

$$\begin{aligned} &163644703763600866631298225238422^{119725983215366906541881876496587} \\ &\equiv 22 \mod 2222222222244444688766666666665544431 \end{aligned}$$

If now we use the number-to-letter equivalents:

S = 083, O = 079, R = 082, T = 084, I = 073, N = 078, G = 071, and the received message is

$$6991924052385460712101963059912 5/13928424360600129492446186572 2675/12976174049741160897711201801 8483$$

the original message is decoded by calculating

$$6991924052385460712101963059912 5^x \equiv 83084 \mod n$$

and

$$1392842436060012949244618657226 75^x \equiv 82079 \mod n$$

and

$$1297617404974116089771120180184 83^x \equiv 78071 \mod n$$

Juxtaposing these blocks gives 083084082079078071, and so the message was the word S T R O N G.

Example 3 Take $p = 212345678987654321$ and $q = 953947941937929919$ to be our two primes p, q. So $n = 202566723449685169430593680295529999$ and

$$\begin{aligned}\phi(n) &= (212345678987654321 - 1)(953947941937929919 - 1)\\ &= 202566723449685168264300059369945760.\end{aligned}$$

We choose an integer a relatively prime to $\phi(n)$: Say $a = 153561503399845956454967606639962441$. Express 1 as a linear combination of $\phi(n)$ and a:

$$140051113584546175392105575891225401 \cdot a - 106169755765474545609016227483415834 \cdot \phi(n) = 1$$

so 'x' is 140051113584546175392105575891225401. We publish

$$(n, a) = (202566723449685169430593680295529999, 153561503399845956454967606639962441)$$

To encode a block β, the sender calculates $\beta^a \mod n$, and to decode a received block m, we calculate $m^x \mod n$.

Thus, for example, to encode the message $\beta = 82$, the sender computes

$$\begin{aligned}&82^{153561503399845956454967606639962441} \mod 202566723449685169430593680295529999\\ &= 85486127368849881359538683139089967 \mod 202566723449685169430593680295529999\end{aligned}$$

and so sends $m = 85486127368849881359538683139089967$. On receipt of this message, anyone who knows 'x' (the inverse of $a \mod n$) computes

$$\begin{aligned}&85486127368849881359538683139089967^{140051113584546175392105575891225401}\\ &\equiv 82 \mod 202566723449685169430593680295529999\end{aligned}$$

If now we use the number-to-letter equivalents from three-digit decimal ASCII encoding:

L = 076, O = 079, G = 071, A = 065, R = 082, I = 073, T = 084, H = 072, M = 077, S = 083,

and the received message is

$$194753998824973598074264734267684810/57760328407234384633409165135532073/89484846973808817159989225376884183/32717708417152903133335873976745661/19265561399985097566511702437606411 7$$

the original message is decoded by calculating

$$194753998824973598074264734267684810^x \equiv 65076 \mod n$$

and

$$57760328407234384633409165135532073^x \equiv 71079 \mod n$$

and

$$89484846973808817159989225376884183^x \equiv 82073 \mod n$$

and

$$32717708417152903133335873976745661^x \equiv 84072 \mod n$$

and

$$192655613999850975665117024376064117^x \equiv 77083 \mod n$$

Juxtaposing these blocks gives 065076071079082073084072077083, and so the message was the word A L G O R I T H M S.