Assignment C

Moldovan Vasilica
Group: 935
mvie2542

Plaintext to encrypt: Mold.

Let $p=29$ and $q=31 \Rightarrow n=899$, and $k=2$, $l=3$.

Then, $\varphi(n)=(p-1)(q-1)=28\cdot 30=840$.

We select $e=89$ such that $1<e<\varphi(n)$ and $(e,\varphi(n))=1$.

For n, we have $27^k<n<27^l \Leftrightarrow 27^2<899<27^3$

We need to compute $d=e^{-1} \bmod \varphi(n)$ to obtain Alice's private key.

We compute $89^{-1} \bmod 840 = 689$ by the extended Euclidean algorithm.

$$840 = 9\cdot 89 + 39$$
$$89 = 2\cdot 39 + 11$$
$$39 = 3\cdot 11 + 6$$
$$11 = 1\cdot 6 + 5$$
$$6 = 1\cdot 5 + 1$$
$$5 = 5\cdot 1.$$

Then, $(840, 89)=1$, hence there exists $89^{-1} \bmod 840$.

We have:

$$1 = 6-1\cdot 5 = 6-(1\cdot 11-1\cdot 6) = 2\cdot 6-1\cdot 11 = 2\cdot(39-3\cdot 11)-1\cdot 11 =$$
$$= 2\cdot 39-7\cdot 11 = 2\cdot 39-7(89-2\cdot 39) = 16\cdot 39-7\cdot 89 = 16\cdot(840-9\cdot 89)-7\cdot 89 =$$
$$= 16\cdot 840-151\cdot 89.$$

Hence $89^{-1} \bmod 840 = -151 \Leftrightarrow 89^{-1} \bmod 840 = 689$.

Then, Alice's public key is $K_E=(n,e)=(899,89)$ and her private key is $K_D=d=689$.

Split the plaintext: mo | ld

Numerical equivalents: 366 328

mo $\rightarrow 13\cdot 27+15=366$

ld $\rightarrow 12\cdot 27+4=328$

Encrypt ($m^e \bmod n$):

$366^{89} \bmod 899 = ?$

We compute this by repeated squaring modular exponentiation.

We have $89=2^0+2^3+2^4+2^6$. Compute modulo 899:

$366^{(2^0)} = 366$

$366^{(2^1)} = 366^{(2^0)} \cdot 366^{(2^0)} = 366 \cdot 366 = 5$
$366^{(2^2)} = 366^{(2^1)} \cdot 366^{(2^1)} = 5 \cdot 5 = 25$
$366^{(2^3)} = 366^{(2^2)} \cdot 366^{(2^2)} = 25 \cdot 25 = 625$
$366^{(2^4)} = 366^{(2^3)} \cdot 366^{(2^3)} = 625 \cdot 625 = 459$
$366^{(2^5)} = 366^{(2^4)} \cdot 366^{(2^4)} = 459 \cdot 459 = 315$
$366^{(2^6)} = 366^{(2^5)} \cdot 366^{(2^5)} = 315 \cdot 315 = 335$

Then, $366^{89} = 366^{2^0+2^3+2^4+2^6} = 366 \cdot 625 \cdot 459 \cdot 335 = 160 \pmod{899}$.

$366^{89} = 160 \pmod{899}$

$328^{89} \bmod 899 = ?$

$328^{(2^0)} = 328$
$328^{(2^1)} = 328^{(2^0)} \cdot 328^{(2^0)} = 328 \cdot 328 = 603$
$328^{(2^2)} = 328^{(2^1)} \cdot 328^{(2^1)} = 603 \cdot 603 = 413$
$328^{(2^3)} = 328^{(2^2)} \cdot 328^{(2^2)} = 413 \cdot 413 = 658$.
$328^{(2^4)} = 328^{(2^3)} \cdot 328^{(2^3)} = 658 \cdot 658 = 545$
$328^{(2^5)} = 328^{(2^4)} \cdot 328^{(2^4)} = 545 \cdot 545 = 355$.
$328^{(2^6)} = 328^{(2^5)} \cdot 328^{(2^5)} = 355 \cdot 355 = 165$.

Then, $328^{89} = 328^{2^0+2^3+2^4+2^6} = 328 \cdot 658 \cdot 545 \cdot 165 = 701 \pmod{899}$

$328^{89} = 701 \pmod{899}$

Then, the result of encryption is 160 701.

The literal equivalents are:

$160 = 0 \cdot 27^2 + 5 \cdot 27 + 25 \Rightarrow$ _EY

$701 = 0 \cdot 27^2 + 25 \cdot 27 + 26 \Rightarrow$ _YZ.

Ciphertext: _EY_YZ

Decription part.

Ciphertext: _EY_YZ

Split the ciphertext: _EY | _YZ

The numerical equivalents are:

_EY $\longrightarrow 0 \cdot 27^2 + 5 \cdot 27 + 25 = 160$

_YZ $\longrightarrow 0 \cdot 27^2 + 25 \cdot 27 + 26 = 701$.

Decription ($c^d \bmod n$)

$160^{689} \bmod 899 = ?$

$689 = 2^0 + 2^4 + 2^5 + 2^7 + 2^9$

$160^{(2^0)} = 160$

$366^{(2^6)} = 366^{(2^5)} \cdot 366^{(2^5)} = $ [illegible]

[illegible] 89 [illegible] $2^0+2^3+2^4+2^6$ [illegible] (mod 899)

$160^{(2^1)} = 160^{(2^0)} \cdot 160^{(2^0)} = 160 \cdot 160 = 428$

$160^{(2^2)} = 160^{(2^1)} \cdot 160^{(2^1)} = 428 \cdot 428 = 687$

$160^{(2^3)} = 160^{(2^2)} \cdot 160^{(2^2)} = 687 \cdot 687 = 893$

$160^{(2^4)} = 160^{(2^3)} \cdot 160^{(2^3)} = 893 \cdot 893 = 36$

$160^{(2^5)} = 160^{(2^4)} \cdot 160^{(2^4)} = 36 \cdot 36 = 397$

$160^{(2^6)} = 160^{(2^5)} \cdot 160^{(2^5)} = 397 \cdot 397 = 284$

$160^{(2^7)} = 160^{(2^6)} \cdot 160^{(2^6)} = 284 \cdot 284 = 645$

$160^{(2^8)} = 160^{(2^7)} \cdot 160^{(2^7)} = 645 \cdot 645 = 687$

$160^{(2^9)} = 160^{(2^8)} \cdot 160^{(2^8)} = 687 \cdot 687 = 893$

$160^{689} = 160^{2^0+2^4+2^5+2^7+2^9} = 160 \cdot 36 \cdot 397 \cdot 645 \cdot 893 = 366 \pmod{899}$.

$701^{689} \bmod 899 = ?$

$701^{(2^0)} = 701$

$701^{(2^1)} = 701^{(2^0)} \cdot 701^{(2^0)} = 701 \cdot 701 = 547$

$701^{(2^2)} = 701^{(2^1)} \cdot 701^{(2^1)} = 547 \cdot 547 = 741$

$701^{(2^3)} = 701^{(2^2)} \cdot 701^{(2^2)} = 741 \cdot 741 = 691$

$701^{(2^4)} = 701^{(2^3)} \cdot 701^{(2^3)} = 691 \cdot 691 = 112$

$701^{(2^5)} = 701^{(2^4)} \cdot 701^{(2^4)} = 112 \cdot 112 = 857$

$701^{(2^6)} = 701^{(2^5)} \cdot 701^{(2^5)} = 857 \cdot 857 = 865$

$701^{(2^7)} = 701^{(2^6)} \cdot 701^{(2^6)} = 865 \cdot 865 = 257$

$701^{(2^8)} = 701^{(2^7)} \cdot 701^{(2^7)} = 257 \cdot 257 = 422$

$701^{(2^9)} = 701^{(2^8)} \cdot 701^{(2^8)} = 422 \cdot 422 = 82$

$701^{689} = 701^{2^0+2^4+2^5+2^7+2^9} = 701 \cdot 112 \cdot 857 \cdot 257 \cdot 82 = 328 \pmod{899}$

The result of decryption is: 366 228.

The literal equivalents are:

$366 = 13 \cdot 27 + 15 \Rightarrow$ mo

$328 = 12 \cdot 27 + 4 \Rightarrow$ ld

Then, we obtain the plaintext: mold.

All the key constraints are respected when constructing the key, so they are valid.