Lecture 3

Enciphering function

$$f: \mathbb{Z}_{37} \to \mathbb{Z}_{37},\ x \mapsto \alpha' x + \beta'$$

over

$0, 1, \ldots, 9, A=10, \ldots, Z=35, \_=36$

Last characters of plaintext:

COMPUTING

Last characters of ciphertext:

. . . . . IO

Deciphering function:

$$g: \mathbb{Z}_{37} \to \mathbb{Z}_{37},\ x \mapsto \alpha x + \beta$$

$g(0) = G$

$g(I) = N$

$$\begin{cases} g(24) = 24\alpha + \beta = 16 \\ g(13) = 13\alpha + \beta = 23 \end{cases} \quad \text{mod } 37$$

Solve

$$\begin{aligned} 24\alpha + \beta &= 16 \\ 13\alpha + \beta &= 23 \end{aligned} \quad \text{mod } 37$$

Taking the second from the first:

$$24\alpha + \beta = 16 \pmod{37}$$

$$6\alpha = -7 = 30$$

so $\boxed{\alpha = 5}$

using $24\alpha + \beta = 16$ we get

$$24(5) + \beta = 16 \pmod{37}$$

$$9 + \beta = 16 \pmod{37}$$

$$\boxed{\beta = 7}$$

The cipher text is

Y 2 V S N ....

" " "

34 2 31 ....

$\boxed{g(x) = 5x + 7}$

The plain text is

g(34) g(2) g(31) ....

" "

29 'T "

" "

T H E

Theorem

- Suppose $n = pq$ with p, q distinct primes.
- suppose e is a number with

$$\text{hcf}(p-1, e) = 1 = \text{hcf}(q-1, e).$$

- Suppose

$$de \equiv 1 \mod \phi(n)$$

Then

$$(x^e)^d \equiv x \mod n.$$

Proof We must show

$$(x^e)^d - x \equiv 0 \mod n.$$

Equivalently we must show

$$(x^{ed-1} - 1)\, x \quad \text{is divisible by } n. \qquad (*)$$

If both p and q divide x the $(*)$ certainly holds.

Suppose then that p does not divide x.

Now

$$de \equiv 1 \mod \phi(n)$$

and thus

$$de - 1 = k\phi(n) \text{ for some } k$$

Working modulo p we have

$$\begin{aligned} x^{de-1} - 1 &= x^{k\phi(n)} - 1 \\ &= \left(x^{p-1}\right)^{k(q-1)} - 1 \\ &\equiv 1^{k(q-1)} - 1 \\ &\equiv 1 - 1 \\ &\equiv 0. \end{aligned} \qquad \text{mod } p$$

Thus p divides $x^{de-1} - 1$.

We must consider two cases.

Case 1 If q divides x then $n = pq$ divides

$$(x^{ed-1} - 1)\, x .$$

Case 2 Suppose q does not divide x. Then, by the above argument for p, we get that q divides

$$x^{ed-1} - 1 .$$

So $n = pq$ divides $x^{ed-1} - 1$ and (*) holds.

Q.E.D.