Loïc Galland
1998 04 13 19 11

1MA464



(5) What we know:

plaintext = Codingtheory

ciphertext = nwqmnxeprsprp

Vigenère encrypting

What we want:

key

We know that Vigenère encrypting works with key being added to the plaintext. So if we take the encryted text and we substract it by the plaintext we should get the key that is repeating.

plaintext: C O D I N G T H E O R Y
2 14 3 8 13 6 19 7 4 14 17 24

Ciphertext: N W Q M N X E P R S R P
13 22 16 12 13 23 4 15 17 18 17 15

N - C = 13 - 2 = 11 → L
W - O = 22 - 14 = 8 → I
Q - D = 16 - 3 = 13 → N
M - I = 12 - 8 = 4 → E
N - N = 13 - 13 = 0 → A
X - G = 23 - 6 = 17 → R
E - T = 4 - 19 = -15 = 11 mod 26 → L
P - H = 15 - 7 = 8 → I
R - E = 17 - 4 = 13 → N
S - O = 18 - 14 = 4 → E
R - R = 17 - 17 = 0 → A
P - Y = 15 - 24 = -9 = 17 mod 26 → R

We can clearly see that the key is

LINEAR

⑦ We know that:

$n = 4891$

the ciphertext is $c = 2$ when the public key $(n, e) = (4891, 1901)$ is used.

We also know that Fermat's Factorization Method was used.

So $n = a^2 - b^2 = (a+b)(a-b) = 4891$.

First we want to check if it is a perfect square.

$\sqrt{4891} \approx 69,93$ → Therefore it is not a perfect square

To find the perfect square, we then need to test values to see what works.

$\sqrt{4891+1^2} \approx 69,94$ → Does not work!

$\sqrt{4891+2^2} \approx 69,96$ → Does not work!

$\sqrt{4891+3^2} = 70$ → Here it works

Therefore we can say that $a = 70$ and $b = 3$

Now we can use a and b in the equation from the beginning

$(70+3)(70-3) = 73 \cdot 67 = \underline{4891}$

Therefore we can see that it works and the factors of 4891 are 73 and 67.

Now to find the plaintext we can use this formula.

$$\text{plaintext} = C^d \bmod n$$

we know that $m = p^T$

$m^e \bmod n = C$

$m \bmod n \equiv C^d$

To be able to find what we need is the decryption key for $(n, e) = (4891, 1901)$

$\varphi(n) = (p-1)(q-1) = (73-1)(67-1) = 4752$

Now we can say that the equation $d \cdot e = 1 \bmod (\varphi(n))$

$d \cdot 1901 = 1 \bmod 4752$

Loïc Galland
19980413 1911

1MA464



⑦ continue

Now we can use the Euclidean algorithm:

$$4752 = (2 \cdot 1901) + 950$$
$$1901 = (950 \cdot 2) + 1$$
$$950 = 1 \cdot 950 + 0$$

Now we can reuse that line with the extended Euclidean algorithm

$$1901 = (950 \cdot 2) + 1$$
$$1901 - (950 \cdot 2) = 1$$
$$1901 - 2(4752 - 2(1901)) = 1$$
$$1901 - 2 \cdot 4752 + 4 \cdot 1901 = 1$$
$$5 \cdot 1901 - 2 \cdot 4752 = 1$$

T e

Therefore now $e \cdot 1901 \Rightarrow d = 5$

So the plaintext $m = c^d \bmod n$
$= 2^5 \bmod 4891$