Theory of encryption algo.

Encoding :

We implement RSA in the polynomial ring $Z_{29}[x]$. That is when encoding the plaintext, the corresponding polynomial will be a member of polynomial ring:

$$Z_{29}[x] = \{a_0 + a_1x + a_2x^2 \cdots - a_kx^k\}, k \geq 0, \quad a_i \in Z_{29}$$

The public key is represented by the pair $(N(x), e)$ and private key represented by the triple $(P(x), Q(x), d)$.

Now it is possible to encode all the letters in the swedish alphabet which contains 29 letters. We see that the reason behind the choice of encoding plaintext into polynomials with coefficients belonging to Z_{29}.

Encoding of Plaintext = It is encoded as a sequence of polynomials of degree smaller than degree of $N(x)$.

$N(x)$ = Product of 2 irreducible polynomials $P(x)$ and $Q(x)$.

* Each letter will be encoded into its corresponding position in the alphabet starting with letter a being a position 0.

Ex. $P(x) = ax^2 + bx + c$

$Q(x) = dx^2 + ex + f$.

Now $N(x) = P(x)\,Q(x)$ = this is a polynomial of ~~degree~~ degree 4.

↳ this means that for the plaintext "hello", blocks of four letters are encoded at a time.

NOTE: IF we cannot make blocks of four (size ↑) letters, we add extra x's ~~until~~ until we can encode.

The plaintext hello will be encoded as a sequence of 2 polynomials namely one corresponding to the first four letters in the plaintext $M_1(x) = 7x^3 + 4x^2 + 11x + 11$ and the other one corresponding to the letter o to which we add 3 x's to make it complete having $M_2(x) = 14x^3 + 23x^2 + 23x + 23$

How we got the coefficients in the polynomial on the previous page?

⇒ we have taken 0-indexing of alphabet

So hello

/ \

hell 0xxx

hell = $7x^3 + 9x^2 + 11x + 11$

0xxx = $14x^3 + 23x^2 + 23x + 23$

Now To get $C_1(x)$, $C_2(x)$ we perform modular exponentiation:

$$C_1(x) = M_1(x)^e \bmod N(x)$$
$$C_2(x) = M_2(x)^e \bmod N(x)$$

C_1 & C_2 represent the ciphertexts whose coefficients represent in order the position in the alphabet of each letter of Plaintext.

Encrypting Process: we have to choose 2 irreducible polynomials. Now we need to calculate N(x) the encryption exponent e will be randomly chosen from the set $Z_S = \{0, 1, 2 \dots S-1\}$, such that $gcd(e, S) = 1$.

Encryption Algorithm :-

Step-1 First we calculate the highest degree of $P(x) \cdot Q(x)$. i.e

n = highest deg. = highest Deg ($P(x)$) + highest Deg ($Q(x)$)

Step-2 We have a string of letters in the message variable, which we need to encrypt.

Step-3 Now, if the message cannot be split into the n no. of terms then we add 'x' in the back till it can be split into n parts.

Ex $n = 4$, message = "hello".
len = 5

$\therefore$ len % n != 0

So, we make len = 8, i.e message = "helloxxx";

Step-4. Now, we store all the $\left(\frac{len}{n}\right)$ parts in an array of strings.

Ex. strings[] = {"hell", "oxxx"};

Step-5 Now we have to calculate the coeff. of plain text and the coeff. of cipher text in their polynomial representation.

Step-6 We will iterate through the strings array and in the array, calculate the alphabetic index of all the characters.

Ex. strings[] = {"hell", "oxxx"};

"hell" → [7,4,11,11]

for each coefficient we calculate the polynomial representing it. i.e $M_i(x)$.

Step-7 Now we have to calculate $C_i(x)$, which is

$$C_i(x) = (M_i(x))^e \% N(x);$$

Step-8 Now to calculate the encrypt message we add the non zero coefficient of $C_i(x)$ in a string str;.

Ex. $P(x) = 19x^3 + 8x^2 + 21x + 5$.
$Q(x) = 21x^3 + 19x^2 + 25x + 2$
, message to encrypt = "izabela".

⇒ $N(x) = 22x^6 + 7x^5 + 24x^4 + 17x^3 + 27x^2 + 22x + 10$
e (public exponent) = 423595285.

⇒ highest deg. of $N(x) = n = 6$

len % n != 0, so len = 12

⇒ izabelaxxxxx

strings[] = {"izabel", "axxxxx"};.
($M_1(x)$ → $C_1(x)$, $M_2(x)$ → $C_2(x)$.)