h(x)=f^(-1)(x)\*g(x) mod q

f(x)\*h(x)=f(x)\*f^(-1)(x)\*g(x) mod q=1\*g(x) mod q= g(x) mod q

f(x)\*h(x)= g(x)+u(x)\*q

f(x)\*h(x)- u(x)\*q = g(x)

f(x)\*1-u(x)\*0=f(x)

f(x)\*(h(x), 1)-u(x)\*(q,0) = (g(x),f(x))

$$\left(f\left(x\right),-u(x)\right)\*\left(\begin{matrix}h\left(x\right)&1\\q&0\end{matrix}\right)=(g(x),f(x))$$

N=3; m(x)=x^3-1;

f(x)=f0+f1\*x+f2\*x^2; h(x)=h0+h1\*x+h2\*x^2;

f(x)\*h(x)=( f0+f1\*x+f2\*x^2)\*( h0+h1\*x+h2\*x^2)= f0\*h0+f0\*h1\*x+f0\*h2\*x^2+ f1\*h0\*x+f1\*h1\*x^2+f1\*h2\*x^3+ f2\*h0\*x^2+f2\*h1\*x^3+f2\*h2\*x^4=

rem(f0\*h0+(f0\*h1+ f1\*h0)\*x +(f0\*h2 +f1\*h1+ f2\*h0)\*x^2+(f1\*h2+f2\*h1)\*x^3+f2\*h2\*x^4,m)=

f0\*h0+(f0\*h1+ f1\*h0)\*x +(f0\*h2 +f1\*h1+ f2\*h0)\*x^2+(f1\*h2+f2\*h1)\*1+rem(f2\*h2\*x^4,m)=

(f0\*h0+f1\*h2+f2\*h1)-q\*u0

(f0\*h1+f1\*h0+f2\*h2)\*x-q\*u1\*x

(f0\*h2 +f1\*h1+ f2\*h0)\*x^2 –q\*u2\*x^2

|  |  |  |
| --- | --- | --- |
| dividend | divisor | quotient |
| x^3-x^3-1 | x^3-1 | 1 |
| 1 rem |  |  |

|  |  |  |
| --- | --- | --- |
| dividend | divisor | quotient |
| x^4-x^4-x | x^3-1 | x |
| X rem |  |  |

f=(f0,f1,f2), h=(h0,h1,h2)

$$f0\*\left(\begin{matrix}h0\\h1\\h2\end{matrix}\right)+f1\*\left(\begin{matrix}h2\\h0\\h1\end{matrix}\right)+f2\*\left(\begin{matrix}h1\\h2\\h0\end{matrix}\right)=$$

$$\left(f0,f1,f2\right)\*\left(\begin{matrix}h0\\h2\\h1\end{matrix}\begin{matrix}h1\\h0\\h2\end{matrix}\begin{matrix}h2\\h1\\h0\end{matrix}\right)-\left(u0,u1,u2\right)\*\left(\begin{matrix}q\\0\\0\end{matrix}\begin{matrix}0\\q\\0\end{matrix}\begin{matrix}0\\0\\q\end{matrix}\right)=$$

$$\left(f0,f1,f2,-u0,-u1,-u2\right)\*\left(\begin{array}{c}\begin{matrix}h0\\h2\\h1\end{matrix}\begin{matrix}h1\\h0\\h2\end{matrix}\begin{matrix}h2\\h1\\h0\end{matrix}\\\begin{matrix}q\\0\\0\end{matrix}\begin{matrix}0\\q\\0\end{matrix}\begin{matrix}0\\0\\q\end{matrix}\end{array}\right)-\left(u0,u1,u2\right)\*\left(\right)$$

x\*qE=qx



A\*V1=a\*(1,0)=(a,0), v2=(0,1)

V1=(1,0), v2=(0,1)=>v=(a,b)=a\*(1,0)+b(0,1)

V1=(v11,v12, .., v1n); v2=(v21,v22, …, v2n)

(v1,v2)=v1\*v2=v11\*v21+v12\*v22+..+v1n\*v2n

||v||=sqrtt(v\*v)=sqrt(v12+ v22+…+ vn2), v=(v1,v2,…,vn)

V1\*=v1

I=2;

$$μ\_{21}=\frac{(v2,v1^{\*})}{\left|\left|v1^{\*}\right|\right|^{2}}=\frac{(v2,v1^{\*})}{(v1^{\*},v1^{\*})}$$

$$v2^{\*}=v2-μ\_{21}v1^{\*}$$

$$(v2^{\*},v1^{\*})=(v2-μ\_{21}v1^{\*},v1^{\*})= (v2,v1^{\*})-(μ\_{21}v1^{\*},v1^{\*})=$$

$$(v2,v1^{\*})-μ\_{21}(v1^{\*},v1^{\*})=$$

$$(v2,v1^{\*})-\frac{(v2,v1^{\*})}{(v1^{\*},v1^{\*})}(v1^{\*},v1^{\*})=$$

$$(v2,v1^{\*})-(v2,v1^{\*})=0$$

I=3

$$μ\_{31}=\frac{(v3,v1^{\*})}{\left|\left|v1^{\*}\right|\right|^{2}}=\frac{(v3,v1^{\*})}{(v1^{\*},v1^{\*})}$$

$$μ\_{32}=\frac{(v3,v2^{\*})}{\left|\left|v2^{\*}\right|\right|^{2}}=\frac{(v3,v2^{\*})}{(v2^{\*},v2^{\*})}$$

$$v3^{\*}=v3-μ\_{31}v1^{\*}-μ\_{32}v2^{\*}$$

$$(v3^{\*},v1^{\*})=(v3-μ\_{31}v1^{\*}-μ\_{32}v2^{\*},v1^{\*})= (v3,v1^{\*})-(μ\_{31}v1^{\*},v1^{\*})-(μ\_{32}v2^{\*},v1^{\*})=$$

$$(v3,v1^{\*})-μ\_{31}(v1^{\*},v1^{\*})-μ\_{32}(v2^{\*},v1^{\*})=(v3,v1^{\*})-\frac{(v3,v1^{\*})}{(v1^{\*},v1^{\*})}(v1^{\*},v1^{\*})=$$

$$(v3,v1^{\*})-(v3,v1^{\*})=0$$

$$\left(a,b\right)=\left|\left|a\right|\right|∙\left|\left|b\right|\right|∙cosφ$$

$$cosφ=\frac{\left(a,b\right)}{\left|\left|a\right|\right|∙\left|\left|b\right|\right|}$$

$$s=\sum\_{i=1}^{n}x\_{i}$$

S=x1;

(For i=2:n){

s=s+xi}

“plaintext” NTRU N=7, p=3, q=41, d=1, f from T(2,1), g from T(1,1), r from T(1,1), plaintext m from Rp => e from Rq p=2=>coefficients are from Z3={0,1,2}; maximal order is 6

[a6,a5,a4,a3,a2,a1,a0] all a’s are from {0,1,2}

2101010=2\*x^6+x^5+x^3+x

ASCII codes? 80, 76, 65, 73, 78, 84, 69, 88, 84=>16x=> 5\*16+0=5016=8010, 4c, 41, 49, 4e, 54, 45, 58, 54=> 010100002 = 64+16=8010 010 01100010000 01 01001001 01001110 01010100 01000101 01001000 01010100

80 10? What it will be in ternary? 2\*3^3+2\*3^2+2\*3+2\*1=0002222 3

P=7 what base will be used?

Number of variants (integers) 3^7=2187

2^10 =>1024; 2^11=2048; 2^12=4096

0010 1000 0010 =282 (16)=>2\*256+8\*16+2=512+128+2=642 (10)

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | Quotient, rem |
| 642 | 3 | 214,0 |
| 214 | 3 | 71,1 |
| 71 | 3 | 23,2 |
| 23 | 3 | 7,2 |
| 7 | 3 | 2,1 |
| 2 | 3 | 0,2 |

0212210=2\*243+1\*81+2\*27+2\*9+1\*3=486+81+54+18+3=567+75=642; 0\*x^6+2\*x^5+x^4+2\*x^3+2\*x^2+x+0\*1

P=>C 22222223=3^7-1=2186=>12 bits ciphertext length =12 bits >plaintext length=11 bits

~~2\*3^5+2\*3^4+0000=2\*243+2\*81=446+162=608~~

detA=a1\*b2-a2\*b1=1\*1-0\*0=1

A=$\left(\begin{matrix}a1&a2\\b1&b2\end{matrix}\right)$

A= (A1=1, a2=0); B= (b1=0, b2=1);

A= (A1=1, a2=0); B= (b1=1, b2=1);

detA=a1\*b2-a2\*b1=1\*1-0\*1=1

0,0

1,0

0,1

RSA

P=47, q=59, n=p\*q=47\*59=2773; fi(n)=(p-1)(q-1)=46\*58=2668

To check for being prime, we divide by all numbers < sqrt(p)=sqrt(47)=6.8; try 2,3,4,5,6

D=157

Extended Euclid algorithm (m modulus, b to be inverted) b^(-1) mod m

A=(A1,A2,A3)=(1,0,m)=(0,1,2668); B=(B1,B2,B3)=(0,1,b)=(0,1,157)

B3=0? If yes, no inverse, A3 is gcd(m,b)<>1, inverse does not exist

B3=1? If yes, inverse is B2, gcd=1

Q=floor(A3/B3)=floor(2668/157)=16

T=A-q\*B=(A1-q\*B1, A2-q\*B2, A3-q\*B3)=(1-16\*0,0-16\*1, 2668-16\*157)=(1,-16,156)

A=B=(0,1,157), B=(1,-16,156)

Q=floor(A3/B3)=floor(157/156)=1

T=A-q\*B=(A1-q\*B1, A2-q\*B2, A3-q\*B3)=(0-1\*1, 1-1\*(-16), 1)=(-1,17,1)

A=B=(1,-16,156); B=(-1,17,1)

B3=1=> B2 =17 is inverse 157^(-1) mod 2668

17\*157= 2669 = 1\*2668+1=1 mod 2668

E=17, d=157

ITS ALL GREEK TO ME

IT Sb AL Lb GR EE Kb TO bM Eb

Zz =>2626

Ba=0001

Blank=01, a=02 => 0102

If coding from 1 to 27, it will fitn=2773

Because the maximal value is 2727<2773

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Blank (b) | a | b | C | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| 00 | 01 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

0920 1900 0112 1200 0718 0505 1100 2015 0013 0500

M1=920

C1=M1^e mod n = 920^17 mod 2773

M1^17 mod n =M^(16+1) mod n=((M^16 mod n)\*M^1) mod n=((M^16 mod n)\*M) mod n

M1^2 mod n = 920^2 mod 2773 = 635

M1^4=(M1^2 mod n)^2 mod n = 635^2 mod 2773=1140

M1^8=1140^2 mod 2773 = 1836

M1^16=1836^2 mod 2773 = 1701

C1=1701\*920 mod 2773 = 948