RSA

N=p\*q, p, q are primes, p<>q

Prime => 2,3,5,7,11,13,17,19,23

Divisible by 1 and by itself; 23=1\*23

Composite=>4=1\*2\*2=2^2;

15=1\*3\*5; 96=1\*2\*2\*2\*2\*2\*3=2^5\*3

A|b A divides b, b is Divisible by A => b/A result is integer

3|15, 15 is divisible by 3; 15=3\*5; 15/3=5.0 integer

 why? 15/4=3.75

C= M^public\_key mod N; M is an integer from ZN

M=2, pk=5, p=3, q=7, N=21; how many bits for 21? 2^4+2^2+2^0=16+4+1=10101; 43210; 2^4 2^3 2^2 2^1 2^0

Private\_key\*public\_key=1 mod fi(N)

Fi(N)=fi(p)\*fi(q)=(p-1)(q-1)=2\*6=12;

Prk\*5=1 mod 12;

x\*5=1 mod 12; x=0, 1,2,3,..,11

p=3; ~~0~~,1,2; 1,2 =>2

q=7; 1,2,3,4,5,6

Prk=pub\_key^(-1) mod fi(N) Euler’s totient function

Relatively prime a,b: gcd(a,b)=1; co-prime

Gcd(2,3)=1;

Gcd(15,20)=5

15=1\*3\*5; 20=1\*2^2\*5

Gcd(20,30)=??10

20=2\*10=2\*2\*5; 30=3\*10=2\*3\*5; 1\*2\*5=10

Extended Euclid algorithm

Rivest Shamir Adleman they got in 2002 Turing prize = Nobel prize

Prk=x=5

M’=C^prk mod N=^5 mod 21

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| X | 1 | 2 | 3 | 4 | 5 |  |  |
| X\*5 mod 12 | 5<>1 | 10<>1 | 15 mod 12=3<>1 | 20 mod 12=8<>1 | 25 mod 12=1==1 |  |  |

C=M^5 mod 21=2^5 mod 21 = 32 mod 21 = ???32 % 21 = 11

Remainder R = A mod B integer from ZB ={0..B-1},

R=A-B\*q=32-21\*1=11; where quotient q=floor(A/B)=floor(32/21)=floor(1+11/21)=1

Ceiling(A/B)= floor(x)<=x<=ceil(x); floor(0.9999975)=0; floor(0.1)=0; ceil(0.1)=1; ceil(0,75)=1

Floor(-0.75)=???-1; ceil(-0.75)=??0

M’=C^prk mod N = 11^5 mod 21 =

11^5= (11^2)^2\*11= p1\*p4 mod 21= 11\*4 mod 21 = 44 mod 21 =2=M plaintext OK

510=4+1=1\*2^2+0\*2^1+1\*2^0=1012

9=>1001=1\*2^3+0\*2^2+0\*2^1+1\*2^0; 8=>1000; 7=>0111; 6=>0110; 5=>0101; 4=>0100; 3=>0011;

2=>0010; 1=>0001; 0=>0000

MSB most significant bit is leftmost

LSB least-significant bit is rightmost

5\*9=45=32+8+4+1=1\*2^5+0\*2^4+1\*2^3+1\*2^2+0\*2^1+1\*2^0=101101 6>4 bits

45 mod 16 =13

45 mod 10 = 5

P1=11 mod 21

P2=11^2 mod 21 =121 mod 21 = (5\*21+16) mod 21 =16

P4=p2^2 mod 21 =16^2 mod 21 = 256 mod 21 = (12\*21+4) mod 21 = (252+4) mod 256 = 4

Polynomial of order n

,

,

1

0

X=0.75

-1

X1=-0.75

In AES GF(2^8) polynomials order 7=8-1; coefficients from Z2={0,1}

Field => multiplicative inverse exist for each element

Rings => no

Addition of polynomials

+=

Multiplication of polynomials

+=

+=

=

=

Order(n)\*order(n)=>order(2n)

A+b+c=(a+b)+c=a+(b+c); associativity addition

A\*b\*c=(a\*b)\*c=a\*(b\*c); associativity multiplication

(A+b)\*x=a\*x+b\*x; right distributivity

X\*(A+b) =x\*a +x\*b; left distributivity

A\*b=b\*a; commutativity; a+b=b+a

0<=R=A mod b < b

R=A –q\*b; q – quotient; q=floor(a/b);

AES=> m(x)=x^8+x^4+x^3+x+1=> GF(2^8)

N=2=> X^2-1=(x-1)(x+1)=x^2-~~x+x~~-1=x^2-1

2^(-1) mod 10 not existing; 2^(-1) mod 10 = x=> x\*2 mod 10=1

3^(-1) mod 10

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 2\*x mod 10 | 0 | 2 | 4 | 6 | 8 | 10 mod 10 =0 | 2 | 4 | 6 | 8 |
| 3\*x mod 10 | 0 | 3 | 6 | 9 | 2 | 5 | 8 | 1 |  |  |

3\*7=1 mod 10 => 3^(-1) mod 10 =7

Gcd(a, mod)=1=>a^(-1) exists, can be found by brute force attacking, or by Extended Euclidean Algorithm

Maple

P=4=1\*2^2; q=9=1\*3^2; q>>p; q>p

Gcd(4,9)=1; relatively prime; co-prime

; congruency=> 1 mod 10 = 11 mod 10=1? Negative ??-39,-29,-19,-9, 1, 11, 21, 31, 41 = class 1; -1 mod 10 =? ??A=-1; B=10; q=floor(-1/10)=floor(-0.1)=???-1

R=-1-10\*(-1)=??-1+10=9

R1=-9-10\*floor(-9/10)= -9-10\*floor(-0.9)= -9-10\*(-1)=-9+10=1

-1, 9,19,29,39

6=>??~~3~~?q=10; 6-q=6-10=???-4

[-5, 5]

-7=>-7+10=3

% mod

Sqrt(10/2)=sqrt(5)=2.23 f=2

X(1)==Y(1)=>true

X(1)==Y(11)=>false; X(1)!=Y(11)=>true

A(x)=3x^4+2x^3+1; B(x)=x^3-1; N=3

R=A mod B=??

Q=quotient(A(x)/B(x))

R=a-q\*b; a=q\*divisor+R

3x^4+2x^3+1/x^3-1; N=3

|  |  |  |
| --- | --- | --- |
| Dividend | Divisor | quotient |
| 3x^4+2x^3+1-3x^4-3x= | 1\*x^3-1 | 3x+2=quotient |
| 2x^3+3x+1-2x^3-2 |  |  |
| 3x+3=remainder=[3,3,0] |  |  |
|  |  |  |

3x^4+2x^3+1=(3x+2)\*( 1\*x^3-1)+ 3x+3=3X^4+2x^3~~-3x~~-2+~~3x~~+3=3X^4+2x^3+1=[1,0,0,2,3]

X^5-x^3+1=[1,0,0,-1,0,1]; N=6

X^4+X^3-x=[0,-1,0,1,1,0] from T(2,1), d=1; T(d+1,d)