

[> restart,

▼ Sous-ensembles

```
> Parcourt := proc(n)
  local E, F, i, j, k, l, t, c, d;
  E := {seq([i], i=1..n)};
  for l from 1 to n-1 do
    t := nops(E);
    print(t, binomial(n, l));
    F := {};
    for i from 1 to t do
      c := E[i][l];
      for k from c+1 to n do
        F := F union {[seq(E[i][m], m=1..l), k]}
      od;
    od;
    E := F;
  od;
end;
> Parcourt(15);
15, 15
105, 105
455, 455
1365, 1365
3003, 3003
5005, 5005
6435, 6435
6435, 6435
5005, 5005
3003, 3003
1365, 1365
455, 455
105, 105
15, 15
{[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]} (1.1)
> ?Isirreduct
> randpoly(x, degree=5, dense);
77 + 91 x5 + 68 x4 - 10 x3 + 31 x2 - 51 x (1.2)
> P := % mod 3;
P := 2 + x5 + 2 x4 + 2 x3 + x2 (1.3)
> Irreduc(P) mod 3;
true (1.4)
```



Un système résistant

```

> Partage := proc(n, p, s, t)
  local i, a, h, j, P;
  h := rand(0..p-1);
  a := array(1..n-1);
  for j from 1 to n-1 do
    a[j] := h();
  P := s + add(a[k].xk, k=1..n-1)
  od;
  i := [seq(subs(x=t[l], P) mod p, l=1..n)];
  end:
> t := [seq(i, i=1..20)];
      t := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20]

```

(2.1)

```

> X := Partage(20, 23, 15, t);
      X := [16, 17, 13, 7, 15, 12, 16, 22, 11, 16, 1, 22, 12, 21, 9, 10, 13, 19, 9, 16]

```

(2.2)

```

> Secret := proc(n, p, t, X)
  local P;
  P := Interp(t, X, x) mod p;
  subs(x=0, P)
  end:
> Secret(20, 23, t, X);

```

15

(2.3)

```

> Partage2 := proc(n, p, m, b, s, t)
  local i, a, h, j, P;
  a := array(1..n-1);
  for j from 1 to n-1 do
    a[j] := subs(x=b, randpoly(x, degree=m-1, dense, coeffs=rand(0..p-1)));
  P := s + add(a[k].xk, k=1..n-1)
  od;
  i := [seq(evala(subs(x=t[l], P) mod p) mod p, l=1..n)];
  end:

```

```

> PolyIrr := proc(p, m)
  local Q, r, c;
  r := false;
  c := 0;
  while r = false do
    Q := xm + randpoly(x, degree=m-1, dense, coeffs=rand(0..p-1));
    r := Irreduc(Q) mod p;
    c := c + 1
  od;
  [Q, c];
  end:

```

> 2⁸;

> *PolyIrr*(2, 256);

$$\begin{aligned}
 & [1 + x^{94} + x^{17} + x^{196} + x^{190} + x^{88} + x^{176} + x^{109} + x^{102} + x^{209} + x^{145} + x^{150} + x^{223} \\
 & + x^{210} + x^{201} + x^{248} + x^{246} + x^{151} + x^{44} + x^{256} + x^{250} + x^{46} + x^{226} + x^{205} \\
 & + x^{194} + x^{182} + x^{156} + x^{139} + x^{55} + x^{180} + x^5 + x^3 + x^{50} + x^{47} + x^{45} + x^{42} \\
 & + x^{37} + x^{35} + x^{33} + x^{32} + x^{31} + x^{30} + x^{26} + x^{25} + x^{22} + x^{12} + x^7 + x^{100} + x^{97} \\
 & + x^{95} + x^{93} + x^{87} + x^{86} + x^{84} + x^{83} + x^{81} + x^{80} + x^{79} + x^{77} + x^{75} + x^{74} + x^{73} \\
 & + x^{72} + x^{70} + x^{69} + x^{67} + x^{66} + x^{64} + x^{62} + x^{60} + x^{59} + x^{54} + x^{237} + x^{172} \\
 & + x^{167} + x^{161} + x^{119} + x^{252} + x^{251} + x^{247} + x^{244} + x^{240} + x^{239} + x^{238} + x^{234} \\
 & + x^{233} + x^{231} + x^{228} + x^{227} + x^{225} + x^{221} + x^{220} + x^{219} + x^{218} + x^{213} + x^{207} \\
 & + x^{203} + x^{198} + x^{197} + x^{195} + x^{193} + x^{184} + x^{183} + x^{178} + x^{175} + x^{174} + x^{171} \\
 & + x^{164} + x^{153} + x^{147} + x^{146} + x^{143} + x^{141} + x^{137} + x^{136} + x^{134} + x^{131} + x^{129} \\
 & + x^{128} + x^{127} + x^{126} + x^{125} + x^{123} + x^{120} + x^{118} + x^{116} + x^{110} + x^{107} + x^{106} \\
 & + x^{104} + x^{103} + x^{254} + x^{101}, 242]
 \end{aligned}
 \tag{2.5}$$

> *PolyIrr*(3, 64);

$$\begin{aligned}
 & [2 + x^{17} + x^{41} + 2x^{11} + 2x^{44} + 2x^{46} + 2x^{55} + 2x^5 + x^4 + x^2 + x^6 + x^{50} + 2x^{48} \\
 & + 2x^{47} + x^{45} + x^{43} + x^{39} + x^{37} + 2x^{36} + x^{35} + x^{33} + x^{32} + 2x^{30} + x^{28} + x^{26} \\
 & + 2x^{25} + x^{24} + 2x^{23} + 2x^{21} + 2x^{20} + 2x^{19} + 2x^{15} + x^{14} + x^{12} + x^9 + x^7 + x^{64} \\
 & + x^{62} + x^{61} + x^{59} + 2x^{58} + x^{57} + 2x^{53} + 2x^{51} + 2x^{63} + 2x^8, 20]
 \end{aligned}
 \tag{2.6}$$

> $q := \text{PolyIrr}(2, 6)[1];$

$$q := x^6 + 1 + x^5 + x^2 + x \tag{2.7}$$

> $\text{alias}(b = \text{RootOf}(q, x) \bmod 2);$

$$b \tag{2.8}$$

> *Choixt* := **proc**(n, p, m, b)

local $t, r;$

$r := 0;$

while $r < n$ **do**

$t := \{\text{seq}(\text{subs}(x = b, \text{randpoly}(x, \text{degree} = m - 1, \text{dense}, \text{coeffs} = \text{rand}(0..p - 1))), i$
 $= 1..2 \cdot n)\} \text{ minus } \{0\};$

$r := \text{nops}(t);$

od;

$t := [\text{seq}(t[i], i = 1..n)];$

end;

> $t := \text{Choixt}(40, 2, 6, b);$

$$\begin{aligned}
 t := & [1, b^2, b^3, b^4, 1 + b^3, 1 + b^4, 1 + b^5, 1 + b, b^2 + 1, b^2 + b, b^3 + b^2, b^3 + b, b^4 \\
 & + b^2, b^4 + b^3, b^5 + b^4, b^5 + b, 1 + b^3 + b, 1 + b^4 + b^2, 1 + b^5 + b^2, 1 + b^5 \\
 & + b^3, 1 + b^5 + b^4, 1 + b^5 + b, b^3 + b^2 + b, b^4 + b^2 + b, b^4 + b^3 + b^2, b^5 + b^3
 \end{aligned}
 \tag{2.9}$$

```

+ b, b5 + b4 + b2, b5 + b4 + b3, b5 + b4 + b, 1 + b3 + b2 + b, 1 + b4 + b2 + b,
1 + b4 + b3 + b2, 1 + b4 + b3 + b, 1 + b5 + b2 + b, 1 + b5 + b3 + b2, 1 + b5
+ b3 + b, 1 + b5 + b4 + b, b4 + b3 + b2 + b, b5 + b3 + b2 + b, b5 + b4 + b2
+ b]

```

```

> s := subs(x = b, randpoly(x, degree = 5, dense, coeffs = rand(0..1)));
      s := b4 + b3 + b2 + b

```

(2.10)

```

> X := Partage2(40, 2, 6, b, s, t);
X := [b3 + b2 + b, b5 + b4 + b3 + b, 1 + b5 + b3 + b2 + b, b5 + b4 + b, 0, b4 + b3
+ b, b5 + b2 + b, b5, b5 + b4, b5 + b3 + b2 + b, 1 + b4 + b2 + b, b4, 1 + b4 + b3
+ b2, b3 + b, 1 + b4 + b2, b5, b4 + b2 + b, 1 + b5 + b2, 1 + b5 + b3 + b2 + b, 1
+ b5 + b, b5 + b2, 1 + b5 + b4 + b, 1 + b5 + b2, 1 + b4 + b3 + b2, b5 + b4
+ b2, b5 + b4 + b3 + b, 0, b5 + b4 + b2, b5 + b3 + b, b5 + b, b2 + b + 1, b4 + b3
+ b2, 1 + b4 + b2 + b, b5 + b3, b4 + b3 + b2, b, b4, b5 + b4 + b3 + b, 1 + b4
+ b, 1 + b4 + b2]

```

(2.11)

```

> Secret2 := proc(n, p, b, t, X)
  local P;
  P := evala(Interp(t, X, x) mod p) mod p;
  evala(subs(x = 0, P)) mod p
end;
> Secret2(40, 2, b, t, X);
      b4 + b3 + b2 + b

```

(2.12)

Partage de secret avec seuil

```

> PSeuil := proc(n, k, p, s, t)
  local i, a, h, j, P;
  h := rand(0..p-1);
  a := array(1..k-1);
  for j from 1 to k-1 do
    a[j] := h();
  P := s + add(a[l]·xl, l = 1..k-1)
  od;
  i := [seq(subs(x = t[l], P) mod p, l = 1..n)];
end;

```

Première méthode de décodage

```

> SecretSeuil := proc(n, k, p, t, X)
  local E, F, G, H, N, i, j, l, c, P, T, Y, b, taille;
  P := Interp(t, X, x) mod p;
  if degree(P, x) < k then return [subs(x = 0, P), 0] fi;

```

```

E := { seq([i], i=1..n) };
N := { seq(i, i=1..n) };
for b from 1 to n do
  H := N minus { E[b][1] };
  Y := [ seq(X[H[a]], a=1..n-1) ];
  T := [ seq(t[H[a]], a=1..n-1) ];
  P := Interp(T, Y, x) mod p;
  if degree(P, x) < k then return [ subs(x=0, P), [b] ] fi;
od;
for l from 1 to floor( $\frac{(n-k)}{2}$ ) do
  print(l);
  taille := nops(E);
  F := { };
  for i from 1 to taille do
    c := E[i][l];
    for b from c+1 to n do
      G := [ seq(E[i][m], m=1..l), b ];
      H := N minus { op(G) };
      Y := [ seq(X[H[a]], a=1..n-l-1) ];
      T := [ seq(t[H[a]], a=1..n-l-1) ];
      P := Interp(T, Y, x) mod p;
      if degree(P, x) < k then return [ subs(x=0, P), G ] fi;
      F := F union { G };
    od;
  od;
  E := F;
end;

```

```
> t := [ seq(i, i=1..20) ];
      t := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20] (3.1.1)
```

```
> X := PSeuil(20, 18, 23, 15, t);
      X := [16, 3, 7, 8, 4, 17, 0, 12, 21, 0, 20, 5, 12, 8, 3, 14, 16, 19, 21, 12] (3.1.2)
```

```
> SecretSeuil(20, 18, 23, t, X);
      [15, 0] (3.1.3)
```

```
> XX := X;
      XX := [16, 3, 7, 8, 4, 17, 0, 12, 21, 0, 20, 5, 12, 8, 3, 14, 16, 19, 21, 12] (3.1.4)
```

```
> XX[7] := 3;
      XX7 := 3 (3.1.5)
```

```
> X := PSeuil(20, 12, 23, 15, t);
      X := [0, 7, 8, 16, 4, 22, 20, 14, 19, 2, 11, 11, 5, 11, 1, 0, 9, 13, 10, 17] (3.1.6)
```

```
> XX := X; XX[5] := 1; XX[6] := 0; XX[20] := 3;
      XX := [0, 7, 8, 16, 4, 22, 20, 14, 19, 2, 11, 11, 5, 11, 1, 0, 9, 13, 10, 17]
      XX5 := 1
```

$$\begin{aligned} \mathcal{X}_6 &:= 0 \\ \mathcal{X}_{20} &:= 3 \end{aligned} \tag{3.1.7}$$

> *SecretSeuil* (20, 12, 23, t , \mathcal{X});

$$\begin{aligned} &1 \\ &2 \\ &[15, [5, 6, 20]] \end{aligned} \tag{3.1.8}$$

▼ Seconde méthode de décodage

> *Equation* := **proc**(m, k, l, p, X, Y)
local $P, Q1, Q2, E, q1, q2, R, S, d, v$;
 $Q1 := \text{add}(q1[i] \cdot x^i, i=0 \dots m-1-l)$;
 $Q2 := \text{add}(q2[i] \cdot x^i, i=0 \dots m-l-k)$;
 $E := \{ \text{seq}(\text{subs}(x=X[j], Q1) + Y[j] \cdot \text{subs}(x=X[j], Q2) \bmod p = 0, j=1 \dots m) \}$;
 $S := \text{solve}(E) \bmod p$;
 $\text{assign}(S)$;
 $v := [[\text{seq}(q1[i], i=0 \dots m-1-l)], [\text{seq}(q2[i], i=0 \dots m-l-k)]]$;
 $q1 := 'q1'; q2 := 'q2'$;
 v ;
end:

> *Decode* := **proc**(m, k, l, p, X, Y)
local $v, E, R, S, Q1, Q2, P, d, r$;
 $v := \text{Equation}(m, k, l, p, X, Y)$;
 $Q1 := \text{add}(v[1][i] \cdot x^{i-1}, i=1 \dots m-l)$;
 $Q2 := \text{add}(v[2][i] \cdot x^{i-1}, i=1 \dots m-l-k+1)$;
 $R := \text{Rem}(Q1, Q2, x, P) \bmod p$;
 $r := \text{subs}(x=0, -P \bmod p)$;
end:

> *Decode* := **proc**(m, k, l, p, X, Y)
local $P, Q1, Q2, E, q1, q2, R, S, d, v, i, ni, h, j, r, spe$;
 $Q1 := \text{add}(q1[i] \cdot x^i, i=0 \dots m-1-l)$;
 $Q2 := \text{add}(q2[i] \cdot x^i, i=0 \dots m-l-k)$;
 $E := \{ \text{seq}(\text{subs}(x=X[j], Q1) + Y[j] \cdot \text{subs}(x=X[j], Q2) \bmod p = 0, j=1 \dots m) \}$;
 $S := \text{solve}(E) \bmod p$;
 $Q1 := \text{subs}(S, Q1); Q2 := \text{subs}(S, Q2)$;
 $i := \text{indets}([Q1, Q2])$;
 $ni := \text{nops}(i)$;
 $h := \text{rand}(0 \dots p-1)$;
 $r := 0$;
while $r = 0$ **do**
 for j **from** 2 **to** ni **do**
 $spe := h()$;
 $Q1 := \text{subs}(i[j] = spe, Q1)$;

```

    Q2 := subs(i[j] = spe, Q2);
  od;
  r := Q2;
od;
P := -Quo(Q1, Q2, x) mod p;
subs(x = 0, P);
end:

```

$$\begin{aligned} > t := [seq(i, i = 1..8)]; \\ & \qquad \qquad \qquad t := [1, 2, 3, 4, 5, 6, 7, 8] \end{aligned} \quad (3.2.1)$$

$$\begin{aligned} > X := PSeuil(8, 6, 11, 3, t); \\ & \qquad \qquad \qquad X := [5, 7, 6, 5, 6, 3, 8, 0] \end{aligned} \quad (3.2.2)$$

$$\begin{aligned} > XX := X; XX[1] := 0; \\ & \qquad \qquad \qquad XX := [5, 7, 6, 5, 6, 3, 8, 0] \\ & \qquad \qquad \qquad XX_1 := 0 \end{aligned} \quad (3.2.3)$$

```

> Q1 := add(q1[i]·xi, i = 0..6);
  Q2 := add(q2[i]·xi, i = 0..1);
  E := {seq(subs(x = t[j], Q1) + XX[j]·subs(x = t[j], Q2) mod 11 = 0, j = 1
    ..8)}; nops(E);

```

$$Q1 := q1_0 + q1_1 x + q1_2 x^2 + q1_3 x^3 + q1_4 x^4 + q1_5 x^5 + q1_6 x^6$$

$$Q2 := q2_0 + q2_1 x$$

$$\begin{aligned} E := \{q1_0 + q1_1 + q1_2 + q1_3 + q1_4 + q1_5 + q1_6 = 0, q1_0 + 2q1_1 + 4q1_2 + 8q1_3 \\ + 5q1_4 + 10q1_5 + 9q1_6 = 0, q1_0 + 3q1_1 + 9q1_2 + 5q1_3 + 4q1_4 + q1_5 \\ + 3q1_6 = 0, q1_0 + 4q1_1 + 5q1_2 + 9q1_3 + 3q1_4 + q1_5 + 4q1_6 + 7q2_0 + 6q2_1 \\ = 0, q1_0 + 5q1_1 + 3q1_2 + 4q1_3 + 9q1_4 + q1_5 + 5q1_6 + 5q2_0 + 3q2_1 = 0, q1_0 \\ + 6q1_1 + 3q1_2 + 7q1_3 + 9q1_4 + 10q1_5 + 5q1_6 + q2_0 + 6q2_1 = 0, q1_0 \\ + 7q1_1 + 5q1_2 + 2q1_3 + 3q1_4 + 10q1_5 + 4q1_6 + q2_0 + 7q2_1 = 0, q1_0 \\ + 8q1_1 + 9q1_2 + 6q1_3 + 4q1_4 + 10q1_5 + 3q1_6 + 8q2_0 + 9q2_1 = 0\} \end{aligned} \quad (3.2.4)$$

$$\begin{aligned} > S := solve(E) mod 11; \\ S := \{q1_0 = 8q2_0, q1_1 = 2q2_0, q1_2 = 9q2_0, q1_3 = 7q2_0, q1_4 = 8q2_0, q1_5 = 8q2_0, q1_6 \\ = 2q2_0, q2_0 = q2_0, q2_1 = 10q2_0\} \end{aligned} \quad (3.2.5)$$

$$\begin{aligned} > assign(S); \\ > q1[0]; \\ & \qquad \qquad \qquad 8q2_0 \end{aligned} \quad (3.2.6)$$

$$\begin{aligned} > indets([Q1, Q2]); \\ & \qquad \qquad \qquad \{x, q2_0\} \end{aligned} \quad (3.2.7)$$

```

> Q1, Q2;

```

$$8 q_2^0 + 2 q_2^0 x + 9 q_2^0 x^2 + 7 q_2^0 x^3 + 8 q_2^0 x^4 + 8 q_2^0 x^5 + 2 q_2^0 x^6$$

$$q_2^0 + 10 q_2^0 x \quad (3.2.8)$$

> $Q1 := \text{subs}(q2[0]=1, Q1); Q2 := \text{subs}(q2[0]=1, Q2);$
 $Q1 := 8 + 2x + 9x^2 + 7x^3 + 8x^4 + 8x^5 + 2x^6$
 $Q2 := 1 + 10x$ (3.2.9)

> $R := \text{Rem}(Q1, Q2, x, 'P') \bmod 11;$
 $R := 0$ (3.2.10)

> $-P \bmod 11;$
 $3 + x + 3x^2 + 7x^3 + 10x^4 + 2x^5$ (3.2.11)

> $q1 := 'q1'; q2 := 'q2';$
 $q1 := q1$
 $q2 := q2$ (3.2.12)

> $\text{Decode}(8, 6, 1, 11, t, XX);$
 3 (3.2.13)

> $X := \text{PSeuil}(8, 4, 11, 3, t);$
 $X := [3, 5, 1, 5, 9, 5, 7, 7]$ (3.2.14)

> $XX := X; XX[1] := 1; XX[5] := 5;$
 $XX := [3, 5, 1, 5, 9, 5, 7, 7]$
 $XX_1 := 1$
 $XX_5 := 5$ (3.2.15)

> $\text{Decode}(8, 4, 2, 11, t, XX);$
 3 (3.2.16)

> $t := [\text{seq}(i, i=1..8)];$
 $t := [1, 2, 3, 4, 5, 6, 7, 8]$ (3.2.17)

> $X := \text{PSeuil}(8, 4, 11, 3, t);$
 $X := [0, 3, 3, 2, 2, 5, 2, 6]$ (3.2.18)

> $XX := X; XX[1] := 1;$
 $XX := [0, 3, 3, 2, 2, 5, 2, 6]$
 $XX_1 := 1$ (3.2.19)

> $\text{Decode}(8, 4, 2, 11, t, XX);$
 3 (3.2.20)

> $t := [\text{seq}(i, i=1..20)];$
 $t := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20]$ (3.2.21)

> $X := \text{PSeuil}(20, 12, 23, 3, t);$
 $X := [11, 7, 6, 7, 7, 11, 6, 22, 2, 4, 12, 10, 13, 9, 3, 22, 18, 22, 4, 5]$ (3.2.22)

> $XX := X; XX[1] := 1; XX[5] := 1; XX[20] := 0;$
 $XX := [11, 7, 6, 7, 7, 11, 6, 22, 2, 4, 12, 10, 13, 9, 3, 22, 18, 22, 4, 5]$
 $XX_1 := 1$

$$XX_5 := 1$$

$$XX_{20} := 0 \quad (3.2.23)$$

```
> Decode(20, 12, 3, 23, t, XX);
```

$$3 \quad (3.2.24)$$

Plus de menteurs

Exemple 1. $m=26, k=7, \text{delta}=2, l<12$.

```
> t := [seq(i, i=1..26)];
```

```
t := [1, 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] (3.3.1.1)
```

```
> X := PSeuil(26, 7, 29, 15, t);
```

```
X := [17, 6, 16, 18, 5, 17, 19, 9, 8, 19, 13, 0, 11, 20, 9, 2, 10, 3, 25, 17, 15, 27, 24, 16, 10, 24] (3.3.1.2)
```

```
> h := rand(0..28);
```

```
h := proc( ) (3.3.1.3)
```

```
proc( ) option builtin = RandNumberInterface, end proc(6, 29, 5)
```

```
end proc
```

```
> XX := X; for i from 1 to 11 do XX[i] := h( ) od;
```

```
XX := [17, 6, 16, 18, 5, 17, 19, 9, 8, 19, 13, 0, 11, 20, 9, 2, 10, 3, 25, 17, 15, 27, 24, 16, 10, 24]
```

$$XX_1 := 15$$

$$XX_2 := 0$$

$$XX_3 := 5$$

$$XX_4 := 12$$

$$XX_5 := 13$$

$$XX_6 := 6$$

$$XX_7 := 27$$

$$XX_8 := 6$$

$$XX_9 := 2$$

$$XX_{10} := 13$$

$$XX_{11} := 28 \quad (3.3.1.4)$$

```
> Q := add(add(q[i,j]·xi·yj, i=0..14-6·j), j=0..2);
```

```
Q := q5,1 x5 y + q2,2 x2 y2 + q7,0 x7 + q1,2 x y2 + q8,1 x8 y + q2,0 x2 + q1,1 x y (3.3.1.5)
```

$$+ q_{12,0} x^{12} + q_{3,0} x^3 + q_{9,0} x^9 + q_{1,0} x + q_{7,1} x^7 y + q_{5,0} x^5 + q_{0,1} y$$

$$+ q_{4,1} x^4 y + q_{0,2} y^2 + q_{11,0} x^{11} + q_{6,1} x^6 y + q_{10,0} x^{10} + q_{8,0} x^8$$

$$+ q_{4,0} x^4 + q_{3,1} x^3 y + q_{6,0} x^6 + q_{2,1} x^2 y + q_{13,0} x^{13} + q_{0,0} + q_{14,0} x^{14}$$

> $E := \{seq(subs(x=t[i], subs(y=XX[i], Q)) \bmod 29 = 0, i=1..26)\} :$

> $S := solve(E) \bmod 29;$

$$S := \{q_{0,0} = 0, q_{0,1} = 10 q_{7,0}, q_{0,2} = 9 q_{7,0}, q_{1,0} = 21 q_{7,0}, q_{1,1} = 25 q_{7,0}, q_{1,2} = q_{7,0}, q_{2,0} = 21 q_{7,0}, q_{2,1} = 16 q_{7,0}, q_{2,2} = 14 q_{7,0}, q_{3,0} = 4 q_{7,0}, q_{3,1} = 14 q_{7,0}, q_{4,0} = 5 q_{7,0}, q_{4,1} = 9 q_{7,0}, q_{5,0} = 24 q_{7,0}, q_{5,1} = 17 q_{7,0}, q_{6,0} = 10 q_{7,0}, q_{6,1} = 4 q_{7,0}, q_{7,0} = q_{7,0}, q_{7,1} = 25 q_{7,0}, q_{8,0} = 21 q_{7,0}, q_{8,1} = 11 q_{7,0}, q_{9,0} = 4 q_{7,0}, q_{10,0} = 21 q_{7,0}, q_{11,0} = 28 q_{7,0}, q_{12,0} = 18 q_{7,0}, q_{13,0} = 28 q_{7,0}, q_{14,0} = 27 q_{7,0}\} \quad (3.3.1.6)$$

> $Q := subs(S, Q);$

$$Q := 21 q_{7,0} x^2 + 18 q_{7,0} x^{12} + 4 q_{7,0} x^3 + 4 q_{7,0} x^9 + 21 q_{7,0} x + 24 q_{7,0} x^5 + 10 q_{7,0} y + 9 q_{7,0} y^2 + 28 q_{7,0} x^{11} + 21 q_{7,0} x^{10} + 21 q_{7,0} x^8 + 5 q_{7,0} x^4 + 10 q_{7,0} x^6 + 28 q_{7,0} x^{13} + 27 q_{7,0} x^{14} + q_{7,0} x^7 + 25 q_{7,0} x^7 y + 9 q_{7,0} x^4 y + 17 q_{7,0} x^5 y + 25 q_{7,0} x y + 16 q_{7,0} x^2 y + 14 q_{7,0} x^3 y + 4 q_{7,0} x^6 y + 11 q_{7,0} x^8 y + q_{7,0} x y^2 + 14 q_{7,0} x^2 y^2 \quad (3.3.1.7)$$

> $Q := subs(q[7,0]=1, Q);$

$$Q := 21 x + 10 y + 5 x^4 + 18 x^{12} + 27 x^{14} + 9 y^2 + 9 y x^4 + 16 y x^2 + 25 x y + 14 y^2 x^2 + 11 y x^8 + 4 x^6 y + x y^2 + 17 x^5 y + 14 x^3 y + 21 x^2 + 21 x^8 + 10 x^6 + 24 x^5 + 4 x^3 + 28 x^{13} + 28 x^{11} + 4 x^9 + 21 x^{10} + x^7 + 25 x^7 y \quad (3.3.1.8)$$

> $Q0 := subs(x=0, Q);$

$$Q0 := 10 y + 9 y^2 \quad (3.3.1.9)$$

> $msolve(Q0=0, 29);$

$$\{y=0\}, \{y=15\} \quad (3.3.1.10)$$

> $P := 15;$

$$P := 15 \quad (3.3.1.11)$$

> $dQ := diff(Q, y);$

$$dQ := 10 + 18 y + 9 x^4 + 16 x^2 + 25 x + 28 y x^2 + 11 x^8 + 4 x^6 + 2 x y + 17 x^5 + 14 x^3 + 25 x^7 \quad (3.3.1.12)$$

> $dQP := subs(y=P, dQ) \bmod 29;$

$$dQP := 19 + 9 x^4 + x^2 + 26 x + 11 x^8 + 4 x^6 + 17 x^5 + 14 x^3 + 25 x^7 \quad (3.3.1.13)$$

> $QP := subs(y=P, Q) \bmod 29;$

$$QP := 12 x + 24 x^4 + 18 x^{12} + 27 x^{14} + 18 x^2 + 12 x^8 + 12 x^6 + 18 x^5 + 11 x^3 \quad (3.3.1.14)$$

```

+ 28 x13 + 28 x11 + 4 x9 + 21 x10 + 28 x7
> series ( (QP/dQP), x, 2) mod 29;
22 x + O(x2) (3.3.1.15)
> P := P - convert(%, polynom) mod 29;
P := 15 + 7 x (3.3.1.16)
> dQP := expand(subs(y = P, dQ)) mod 29;
dQP := 19 + 7 x + 9 x4 + 15 x2 + 7 x3 + 11 x8 + 4 x6 + 17 x5 + 25 x7 (3.3.1.17)
> QP := expand(subs(y = P, Q)) mod 29;
QP := 25 x4 + 18 x12 + 27 x14 + 3 x2 + 13 x8 + 15 x6 + 23 x5 + 9 x3 + 28 x13 + 28 x11 + 23 x9 + 21 x10 + 27 x7 (3.3.1.18)
> series ( (QP/dQP), x, 4) mod 29;
20 x2 + 16 x3 + O(x4) (3.3.1.19)
> P := P - convert(%, polynom) mod 29;
P := 15 + 7 x + 9 x2 + 13 x3 (3.3.1.20)
> dQP := expand(subs(y = P, dQ)) mod 29;
dQP := 19 + 7 x + 3 x2 + 27 x3 + 26 x4 + 4 x5 + 11 x8 + 4 x6 + 25 x7 (3.3.1.21)
> QP := expand(subs(y = P, Q)) mod 29;
QP := 23 x4 + 18 x12 + 27 x14 + 26 x8 + 2 x6 + 3 x5 + 28 x13 + 26 x11 + 10 x9 + 10 x10 + x7 (3.3.1.22)
> series ( (QP/dQP), x, 8) mod 29;
18 x4 + 21 x5 + 17 x6 + O(x8) (3.3.1.23)
> P := P - convert(%, polynom) mod 29;
P := 15 + 7 x + 9 x2 + 13 x3 + 11 x4 + 8 x5 + 12 x6 (3.3.1.24)
> expand(subs(y = P, Q)) mod 29;
0 (3.3.1.25)
> expand(subs(y = P, Q));
2175 + 2581 x + 11136 x4 + 6467 x12 + 2175 x14 + 6757 x2 + 18270 x8 + 17429 x6 + 14500 x5 + 8584 x3 + 3248 x13 + 9570 x11 + 14094 x9 + 11803 x10 + 16269 x7 (3.3.1.26)
> discrim(Q, y) mod 29;
x16 + 5 x15 + 13 x14 + 14 x13 + 27 x12 + 13 x11 + 16 x10 + 5 x9 + 23 x8 + 18 x7 + 11 x6 + 14 x5 + 25 x4 + 24 x3 + 18 x2 + 5 x + 13 (3.3.1.27)
> Factor(%) mod 29;
(3.3.1.28)

```

$$(x^4 + 4x^3 + 9x^2 + 25x + 23)^2 (x^4 + 13x^3 + 4x^2 + 20x + 8)^2 \quad (3.3.1.28)$$

> collect(Q, y);

$$(7 + 4x^2 + 22x)y^2 + (18 + x^3 + 13x^7 + 10x^5 + 23x^4 + 4x^2 + 6x + 3x^8 + 16x^6)y + 11 + 24x + 25x^5 + 20x^4 + 23x^{12} + 6x^{14} + 16x^9 + 17x^3 + 19x^{13} + 15x^{11} + 15x^6 + 16x^{10} + 6x^7 + x^8 + 17x^2 \quad (3.3.1.29)$$

▶ **Exemple 2. $m=31, k=5, \text{delta}=3, l<18$.**

> p1 := x⁴ + x + 1;

$$p1 := x^4 + x + 1 \quad (3.3.2.1)$$

> p2 := x⁴ + 2·x² + 2;

$$p2 := x^4 + 2x^2 + 2 \quad (3.3.2.2)$$

> p3 := x⁵ + 3;

$$p3 := x^5 + 3 \quad (3.3.2.3)$$

> QQ := expand((y - p1)·(y - p2)·(y - p3)) mod 37;

$$QQ := 31 + 31x + 11y + 28x^4 + 31y^2 + 9yx^4 + 8yx^2 + 5xy + 35y^2x^4 + 35y^2x^2 + yx^8 + 3x^6y + 36xy^2 + 2x^9y + 4x^5y + 2x^3y + 31x^2 + 32x^8 + 29x^6 + 32x^5 + 31x^3 + y^3 + 36x^{13} + 35x^{11} + 34x^9 + 36x^{10} + 35x^7 + 2x^7y + 36x^5y^2 \quad (3.3.2.4)$$

> degree(QQ, x); degree(QQ, y);

$$\begin{array}{l} 13 \\ 3 \end{array} \quad (3.3.2.5)$$

> $\frac{(3 \cdot 31 - 1)}{4} - 6$;

$$17 \quad (3.3.2.6)$$

> t := [seq(i, i = 1..31)];

$$t := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31] \quad (3.3.2.7)$$

> X := [seq(subs(x = i, p1) mod 37, i = 1..14), seq(subs(x = i, p2) mod 37, i = 15..28), 0, 0, 0];

$$X := [3, 19, 11, 2, 2, 8, 4, 35, 22, 21, 1, 29, 11, 25, 17, 5, 0, 28, 28, 0, 5, 17, 34, 4, 10, 11, 27, 28, 0, 0, 0] \quad (3.3.2.8)$$

> Q := add(add(q[i, j]·xⁱ·y^j, i = 0..13 - 4·j), j = 0..3);

$$Q := q_{5,1}x^5y + q_{2,2}x^2y^2 + q_{7,0}x^7 + q_{3,2}x^3y^2 + q_{1,2}xy^2 + q_{8,1}x^8y + q_{2,0}x^2 + q_{1,1}xy + q_{12,0}x^{12} + q_{3,0}x^3 + q_{5,2}x^5y^2 + q_{9,0}x^9 + q_{1,0}x + q_{1,3}xy^3 + q_{9,1}x^9y + q_{7,1}x^7y + q_{5,0}x^5 + q_{4,2}x^4y^2 + q_{0,1}y + q_{4,1}x^4y + q_{0,3}y^3 + q_{0,2}y^2 + q_{11,0}x^{11} + q_{6,1}x^6y + q_{10,0}x^{10} \quad (3.3.2.9)$$

$$+ q_{8,0} x^8 + q_{4,0} x^4 + q_{3,1} x^3 y + q_{6,0} x^6 + q_{2,1} x^2 y + q_{13,0} x^{13} + q_{0,0}$$

> $E := \{ \text{seq}(\text{subs}(x=t[i], \text{subs}(y=X[i], Q)) \bmod 37 = 0, i=1..31) \}$;

> $S := \text{solve}(E) \bmod 37$;

$$\begin{aligned} S := \{ & q_{0,0} = 30 q_{4,0}, q_{0,1} = 20 q_{4,0}, q_{0,2} = 10 q_{4,0}, q_{0,3} = 14 q_{4,0}, q_{1,0} \\ & = 9 q_{4,0}, q_{1,1} = 32 q_{4,0}, q_{1,2} = 22 q_{4,0}, q_{1,3} = 3 q_{4,0}, q_{2,0} = 3 q_{4,0}, q_{2,1} \\ & = 5 q_{4,0}, q_{2,2} = 3 q_{4,0}, q_{3,0} = 23 q_{4,0}, q_{3,1} = 28 q_{4,0}, q_{3,2} = 4 q_{4,0}, q_{4,0} \\ & = q_{4,0}, q_{4,1} = 14 q_{4,0}, q_{4,2} = 9 q_{4,0}, q_{5,0} = 26 q_{4,0}, q_{5,1} = 9 q_{4,0}, q_{5,2} \\ & = 36 q_{4,0}, q_{6,0} = 22 q_{4,0}, q_{6,1} = 32 q_{4,0}, q_{7,0} = 16 q_{4,0}, q_{7,1} = 13 q_{4,0}, q_{8,0} \\ & = 29 q_{4,0}, q_{8,1} = 14 q_{4,0}, q_{9,0} = 6 q_{4,0}, q_{9,1} = 30 q_{4,0}, q_{10,0} = 2 q_{4,0}, q_{11,0} \\ & = 20 q_{4,0}, q_{12,0} = 0, q_{13,0} = 5 q_{4,0} \} \end{aligned} \quad (3.3.2.10)$$

> $Q := \text{subs}(S, Q)$;

$$\begin{aligned} Q := & q_{4,0} x^4 + 30 q_{4,0} + 3 q_{4,0} x^2 + 23 q_{4,0} x^3 + 6 q_{4,0} x^9 + 9 q_{4,0} x \\ & + 26 q_{4,0} x^5 + 20 q_{4,0} y + 14 q_{4,0} y^3 + 10 q_{4,0} y^2 + 20 q_{4,0} x^{11} \\ & + 2 q_{4,0} x^{10} + 29 q_{4,0} x^8 + 22 q_{4,0} x^6 + 5 q_{4,0} x^{13} + 28 q_{4,0} x^3 y \\ & + 32 q_{4,0} x^6 y + 13 q_{4,0} x^7 y + 5 q_{4,0} x^2 y + 14 q_{4,0} x^8 y + 32 q_{4,0} x y \\ & + 14 q_{4,0} x^4 y + 30 q_{4,0} x^9 y + 36 q_{4,0} x^5 y^2 + 3 q_{4,0} x y^3 + 22 q_{4,0} x y^2 \\ & + 4 q_{4,0} x^3 y^2 + 3 q_{4,0} x^2 y^2 + 9 q_{4,0} x^4 y^2 + 9 q_{4,0} x^5 y + 16 q_{4,0} x^7 \end{aligned} \quad (3.3.2.11)$$

> $Q := \text{subs}(q[4,0]=1, Q)$;

$$\begin{aligned} Q := & 30 + 9 x + 20 y + x^4 + 10 y^2 + 14 y x^4 + 5 y x^2 + 32 x y + 9 y^2 x^4 \\ & + 3 y^2 x^2 + 14 y x^8 + 32 x^6 y + 22 x y^2 + 30 x^9 y + 9 x^5 y + 28 x^3 y + 3 x^2 \\ & + 29 x^8 + 22 x^6 + 26 x^5 + 23 x^3 + 14 y^3 + 5 x^{13} + 20 x^{11} + 6 x^9 + 2 x^{10} \\ & + 16 x^7 + 4 x^3 y^2 + 3 x y^3 + 13 x^7 y + 36 x^5 y^2 \end{aligned} \quad (3.3.2.12)$$

> $Q0 := \text{subs}(x=0, Q)$;

$$Q0 := 30 + 20 y + 10 y^2 + 14 y^3 \quad (3.3.2.13)$$

> $\text{msolve}(Q0=0, 37)$;

$$\{y=1\}, \{y=2\}, \{y=28\} \quad (3.3.2.14)$$

> $\text{Poly} := \text{proc}(Q, y0, n, p)$

local P, dQ, QP, dQP, r, S ;

$r := 1$;

$P := y0$;

$dQ := \text{diff}(Q, y)$;

while $r < n$ **do**

$r := 2 \cdot r$;

$QP := \text{expand}(\text{subs}(y=P, Q)) \bmod p$;

$dQP := \text{expand}(\text{subs}(y=P, dQ)) \bmod p$;

```

S := series ( ( QP / dQP , x , r ) mod p ;
P := P - convert ( S , polynom ) mod p ;
od ;
end :

```

```

> Q - QQ mod 37 ;
36 + 15 x + 9 y + 10 x4 + 16 y2 + 5 y x4 + 34 y x2 + 27 x y + 11 y2 x4
+ 5 y2 x2 + 13 y x8 + 29 x6 y + 23 x y2 + 28 x9 y + 5 x5 y + 26 x3 y + 9 x2
+ 34 x8 + 30 x6 + 31 x5 + 29 x3 + 13 y3 + 6 x13 + 22 x11 + 9 x9 + 3 x10
+ 18 x7 + 4 x3 y2 + 3 x y3 + 11 x7 y

```

(3.3.2.15)

```

> Poly ( Q , 1 , 5 , 37 ) ;
x4 + x + 1

```

(3.3.2.16)

```

> expand ( subs ( y = % , Q ) ) mod 37 ;
0

```

(3.3.2.17)

▼ **Exemple 3. ==31, k=5, delta=3, l<18.**

```

> X := PSeuil ( 31 , 5 , 37 , 3 , t ) ;
X := [ 31 , 15 , 11 , 11 , 17 , 4 , 31 , 19 , 10 , 19 , 34 , 16 , 10 , 34 , 5 , 35 , 24 , 30 , 10 , 5 , 29 , 32 ,
11 , 10 , 9 , 35 , 14 , 30 , 29 , 4 , 32 ]

```

(3.3.3.1)

```

> h := rand ( 0 .. 36 ) ;
h := proc ( )
proc ( ) option builtin = RandNumberInterface , end proc ( 6 , 37 , 6 )
end proc

```

(3.3.3.2)

```

> XX := X ; for i from 1 to 17 do XX [ i ] := h ( ) mod 37 od ;
XX := [ 31 , 15 , 11 , 11 , 17 , 4 , 31 , 19 , 10 , 19 , 34 , 16 , 10 , 34 , 5 , 35 , 24 , 30 , 10 , 5 , 29 ,
32 , 11 , 10 , 9 , 35 , 14 , 30 , 29 , 4 , 32 ]

```

XX₁ := 8

XX₂ := 21

XX₃ := 31

XX₄ := 33

XX₅ := 8

XX₆ := 2

XX₇ := 33

XX₈ := 4

XX₉ := 2

XX₁₀ := 8

XX₁₁ := 23

$$XX_{12} := 36$$

$$XX_{13} := 29$$

$$XX_{14} := 15$$

$$XX_{15} := 28$$

$$XX_{16} := 2$$

$$XX_{17} := 2$$

(3.3.3.3)

> $Q := \text{add}(\text{add}(q[i,j] \cdot x^i \cdot y^j, i=0..13-4 \cdot j), j=0..3);$

$$Q := q_{5,1} x^5 y + q_{2,2} x^2 y^2 + q_{7,0} x^7 + q_{1,2} x y^2 + q_{8,1} x^8 y + q_{2,0} x^2 + q_{1,1} x y \quad (3.3.3.4)$$

$$+ q_{12,0} x^{12} + q_{3,0} x^3 + q_{9,0} x^9 + q_{1,0} x + q_{7,1} x^7 y + q_{5,0} x^5 + q_{0,1} y$$

$$+ q_{4,1} x^4 y + q_{0,2} y^2 + q_{11,0} x^{11} + q_{6,1} x^6 y + q_{10,0} x^{10} + q_{8,0} x^8$$

$$+ q_{4,0} x^4 + q_{3,1} x^3 y + q_{6,0} x^6 + q_{2,1} x^2 y + q_{13,0} x^{13} + q_{0,0} + q_{1,3} x y^3$$

$$+ q_{3,2} x^3 y^2 + q_{9,1} x^9 y + q_{5,2} x^5 y^2 + q_{4,2} x^4 y^2 + q_{0,3} y^3$$

> $E := \{\text{seq}(\text{subs}(x=t[i], \text{subs}(y=XX[i], Q)) \bmod 37 = 0, i=1..31)\};$

> $S := \text{solve}(E) \bmod 37;$

$$S := \{q_{0,0} = 29 q_{2,0}, q_{0,1} = 2 q_{2,0}, q_{0,2} = 7 q_{2,0}, q_{0,3} = 32 q_{2,0}, q_{1,0} = 32 q_{2,0}, \quad (3.3.3.5)$$

$$q_{1,1} = 11 q_{2,0}, q_{1,2} = 21 q_{2,0}, q_{1,3} = 27 q_{2,0}, q_{2,0} = q_{2,0}, q_{2,1} = 36 q_{2,0}, q_{2,2}$$

$$= q_{2,0}, q_{3,0} = 23 q_{2,0}, q_{3,1} = 21 q_{2,0}, q_{3,2} = 21 q_{2,0}, q_{4,0} = 36 q_{2,0}, q_{4,1}$$

$$= 29 q_{2,0}, q_{4,2} = 6 q_{2,0}, q_{5,0} = 35 q_{2,0}, q_{5,1} = 29 q_{2,0}, q_{5,2} = 0, q_{6,0}$$

$$= 8 q_{2,0}, q_{6,1} = 7 q_{2,0}, q_{7,0} = 28 q_{2,0}, q_{7,1} = 17 q_{2,0}, q_{8,0} = 5 q_{2,0}, q_{8,1}$$

$$= 18 q_{2,0}, q_{9,0} = 25 q_{2,0}, q_{9,1} = 17 q_{2,0}, q_{10,0} = 31 q_{2,0}, q_{11,0} = 12 q_{2,0},$$

$$q_{12,0} = 14 q_{2,0}, q_{13,0} = 27 q_{2,0}\}$$

> $Q := \text{subs}(S, Q);$

$$Q := 6 q_{2,0} x^4 y^2 + q_{2,0} x^2 + 29 q_{2,0} + 32 q_{2,0} y^3 + 27 q_{2,0} x^{13} + 8 q_{2,0} x^6 \quad (3.3.3.6)$$

$$+ 36 q_{2,0} x^4 + 5 q_{2,0} x^8 + 31 q_{2,0} x^{10} + 12 q_{2,0} x^{11} + 7 q_{2,0} y^2 + 2 q_{2,0} y$$

$$+ 35 q_{2,0} x^5 + 32 q_{2,0} x + 25 q_{2,0} x^9 + 23 q_{2,0} x^3 + 14 q_{2,0} x^{12}$$

$$+ 28 q_{2,0} x^7 + 7 q_{2,0} x^6 y + 21 q_{2,0} x y^2 + 29 q_{2,0} x^5 y + q_{2,0} x^2 y^2$$

$$+ 11 q_{2,0} x y + 27 q_{2,0} x y^3 + 36 q_{2,0} x^2 y + 17 q_{2,0} x^9 y + 17 q_{2,0} x^7 y$$

$$+ 18 q_{2,0} x^8 y + 21 q_{2,0} x^3 y^2 + 21 q_{2,0} x^3 y + 29 q_{2,0} x^4 y$$

> $Q := \text{subs}(q[2,0]=1, Q);$

$$Q := 29 + 32 x + 2 y + 36 x^4 + 14 x^{12} + 7 y^2 + 29 y x^4 + 36 y x^2 + 11 x y \quad (3.3.3.7)$$

$$+ 6 y^2 x^4 + y^2 x^2 + 18 y x^8 + 7 x^6 y + 21 x y^2 + 17 x^9 y + 29 x^5 y + 21 x^3 y$$

$$+ x^2 + 5x^8 + 8x^6 + 35x^5 + 23x^3 + 32y^3 + 27x^{13} + 12x^{11} + 25x^9$$

$$+ 31x^{10} + 21x^3y^2 + 28x^7 + 17x^7y + 27xy^3$$

> $Q0 := \text{subs}(x=0, Q);$

$$Q0 := 29 + 2y + 7y^2 + 32y^3 \quad (3.3.3.8)$$

> $\text{msolve}(Q0=0, 37);$

$$\{y=3\} \quad (3.3.3.9)$$

> $\text{Poly}(Q, 3, 5, 37);$

$$3 + 23x + 7x^2 + 13x^3 + 22x^4 \quad (3.3.3.10)$$

> $\text{expand}(\text{subs}(y=3, Q)) \bmod 37;$

$$0 \quad (3.3.3.11)$$