TP 5

```
> restart;
```

Mise en place du code

```
> p:=3;m:=5;
```

$$p := 3$$

$$m := 5 \quad (1)$$

```
> P:=X^5+X^4+X^2+1;
```

$$P := X^5 + X^4 + X^2 + 1 \quad (2)$$

```
> alias(alpha=RootOf(P,X) mod p);#définit l'extension K=F_p[alpha]
  de degré m
```

$$\alpha \quad (3)$$

```
> n:=p^m-1; #l'ordre de alpha
```

$$n := 242 \quad (4)$$

la distance apparente du code BCH

```
> delta:=8;
```

$$\delta := 8 \quad (5)$$

le polynôme générateur

```
> g := X^25+X^24+X^22+X^21+X^20+2*X^18+2*X^17+2*X^16+2*X^15+X^13+2*
  X^12+X^10+2*X^8+X^4+X^3+X^2+2*X+1;
```

$$g := X^{25} + X^{24} + X^{22} + X^{21} + X^{20} + 2\,X^{18} + 2\,X^{17} + 2\,X^{16} + 2\,X^{15} + X^{13} + 2\,X^{12} + X^{10} + 2\,X^8 + X^4 + X^3 + X^2 + 2\,X + 1 \quad (6)$$

la dimension

```
> k:=n-degree(g,X);
```

$$k := 217 \quad (7)$$

un exemple de correction

le mot reçu

```
> fr := X^224+X^110+X^109+X^107+X^106+X^105+2*X^103+X^102+X^101+2*
  X^100+2*X^99+X^97+2*X^95+X^94+X^92+2*X^90+2*X^89+X^88+2*X^86+2*
  X^85+X^83+X^82+2*X^81+2*X^78+2*X^77+2*X^76+2*X^74+2*X^73+X^71+2*
  X^70+X^68+2*X^66+2*X^64+2*X^63+X^62+X^59+X^58+X^57+X^56+X^55+
  X^54+2*X^52+X^51+2*X^49+X^47+2*X^43+2*X^42+2*X^41+X^40+2*X^39+2*
  X^19;
```

$$fr := X^{224} + X^{110} + X^{109} + X^{107} + X^{106} + X^{105} + 2X^{103} + X^{102} + X^{101} + 2X^{100} + 2X^{99} + X^{97} + 2X^{95} + X^{94} + X^{92} + 2X^{90} + 2X^{89} + X^{88} + 2X^{86} + 2X^{85} + X^{83} + X^{82} + 2X^{81} + 2X^{78} + 2X^{77} + 2X^{76} + 2X^{74} + 2X^{73} + X^{71} + 2X^{70} + X^{68} + 2X^{66} + 2X^{64} + 2X^{63} + X^{62} + X^{59} + X^{58} + X^{57} + X^{56} + X^{55} + X^{54} + 2X^{52} + X^{51} + 2X^{49} + X^{47} + 2X^{43} + 2X^{42} + 2X^{41} + X^{40} + 2X^{39} + 2X^{19} \quad (8)$$

```
> Rem(fr,g,X) mod p; # le reste n'est pas nul, le mot fr n'est pas
  dans le codegen
```

$$2X^{22} + X^{21} + 2X^{20} + 2X^{19} + X^{18} + 2X^{16} + X^{15} + X^{14} + 2X^{13} + 2X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + 2X^4 + X^3 + 2X^2 + X + 2 \quad (9)$$

le syndrome

```
> S:=sort(add((Expand(subs(X=Power(alpha,i) mod p,fr)) mod p)*X^
  (i-1),i=1..delta-1),X);
```

$$S := \left(\alpha^4 + 2\alpha^2 + \alpha\right)X^6 + \left(2\alpha^4 + 2\alpha^3 + 2\alpha^2 + 2\alpha\right)X^5 + \left(2\alpha^4 + 2\alpha^3 + \alpha + 2\right)X^4 + \left(2\alpha^2 + \alpha\right)X^3 + \left(2\alpha^4 + 2\alpha^3 + 2\alpha^2 + 2\alpha + 1\right)X^2 + \left(2\alpha^4 + \alpha^3 + 2\alpha^2 + 2\alpha + 1\right)X + 2\alpha^4 + 2\alpha + 2 + \alpha^3 + 2\alpha^2 \quad (10)$$

résolution de l'équation clé - algorithme de Euclide-Sugiyama

```
> R0:=X^(delta-1):R1:=S:
> U0:=1:U1:=0:V0:=0:V1:=1:
> do
>    R2:=Rem(R0,R1,X,'Q') mod p;
>    U2:=Expand(U0-Q*U1) mod p;
>    V2:=Expand(V0-Q*V1) mod p;
>    if degree(R2,X) < (delta-1)/2 then break end if;
>    R0, R1 := R1, R2;
>    U0, U1 := U1, U2;
>    V0, V1 := V1, V2;
> end do:
```

```
> R:=collect(R2,X);V:=collect(V2,X);
```

$$R := \left(\alpha^4 + 2\alpha\right)X^2 + \left(2 + 2\alpha + 2\alpha^4\right)X + 2\alpha^2 + 1$$

$$V := \left(2\alpha^4 + \alpha\right)X^3 + \left(2\alpha^3 + \alpha^4 + 2\alpha^2\right)X^2 + \left(\alpha^2 + 2\alpha + 2\alpha^3 + 2\alpha^4 + 2\right)X + 2\alpha^3 + \alpha^2 \quad (11)$$

```
> c:=subs(X=0,V);
```

$$c := 2\alpha^3 + \alpha^2 \quad (12)$$

```
> sigma:=sort(collect(Expand(V/c) mod p,X),X);
```

$$\sigma := \left(2\,\alpha^4 + 2\,\alpha^3 + 1\right) X^3 + \left(\alpha^2 + 2\,\alpha^4 + 2\,\alpha + \alpha^3\right) X^2 + \left(\alpha^2 + 2\,\alpha^4\right) X + 1 \quad \textbf{(13)}$$

```
> omega:=sort(collect(Expand(R/c) mod p,X),X);
```

$$\omega := \left(2 + \alpha^4 + \alpha^3\right) X^2 + \left(2 + 2\,\alpha^4 + \alpha^2\right) X + 2\,\alpha^4 + \alpha^3 + 2\,\alpha^2 + 2\,\alpha + 2 \quad \textbf{(14)}$$

```
> t:=degree(sigma); #il y a t erreurs
```

$$t := 3 \quad \textbf{(15)}$$

l'équation clé est bien satisfaite:

```
> Rem(Expand(S*sigma) mod p -omega ,X^(delta-1),X) mod p;
```

$$0 \quad \textbf{(16)}$$

racines du polynôme localisateur

```
> rc := map( e->e[1],Roots(sigma,alpha) mod p);
```

$$rc := \left[2\,\alpha^4 + \alpha^3,\ \alpha^3 + 2\,\alpha + 1,\ \alpha^4 + 2\,\alpha^3 + \alpha^2 + \alpha + 2\right] \quad \textbf{(17)}$$

calcul du logarithme discret

```
> T:=Array(0..n-1,i->Power(alpha,i) mod p):

> LD:=proc(x)
>   global T,n;
>   local i;
>  for i from 0 to n-1 do
>     if T[i]=x  then return i end if;
>   end do;
> FAIL
> end proc:
```

les degrés des erreurs

```
> d:=map(e->n-e,map(LD,rc));
```

$$d := [19,\ 75,\ 224] \quad \textbf{(18)}$$

formule de Forney

```
> c:=[seq(-Normal(subs(X=rc[j],omega)/subs(X=rc[j],diff(sigma,X)))
  mod p,j=1..t)];
```

$$c := [2,\ 1,\ 1] \quad \textbf{(19)}$$

```
> e:=add(c[i]*X^d[i],i=1..t);
```

$$e := 2\,X^{19} + X^{75} + X^{224} \qquad (20)$$

le mot envoyé

```
> f:=sort(fr-e mod p,X);
```

$$f := X^{110} + X^{109} + X^{107} + X^{106} + X^{105} + 2\,X^{103} + X^{102} + X^{101} + 2\,X^{100} + 2\,X^{99} + X^{97} \qquad (21)$$
$$+ 2\,X^{95} + X^{94} + X^{92} + 2\,X^{90} + 2\,X^{89} + X^{88} + 2\,X^{86} + 2\,X^{85} + X^{83} + X^{82} + 2\,X^{81}$$
$$+ 2\,X^{78} + 2\,X^{77} + 2\,X^{76} + 2\,X^{75} + 2\,X^{74} + 2\,X^{73} + X^{71} + 2\,X^{70} + X^{68} + 2\,X^{66} + 2\,X^{64}$$
$$+ 2\,X^{63} + X^{62} + X^{59} + X^{58} + X^{57} + X^{56} + X^{55} + X^{54} + 2\,X^{52} + X^{51} + 2\,X^{49} + X^{47}$$
$$+ 2\,X^{43} + 2\,X^{42} + 2\,X^{41} + X^{40} + 2\,X^{39}$$

le mot trouvé appartient bien au code et le mot envoyé h

```
> h:=Quo(f,g,X,'r') mod p;r;
```

$$h := X^{85} + 2\,X^{77} + X^{58} + 2\,X^{39}$$

$$0 \qquad (22)$$