...AES...


```
> restart:
> with(numtheory):
>
```

Polinomios

```
> # Um polinómio...
  m:=x^9+x^4+x^3+x+1;
> # ... e a sua factorização módulo 5, ou seja no anel Z_5[X]...
  Factor(m) mod 5;
> #
  # A decomposição em primos (= irredutíveis, neste caso...) de m
  (x)
  # módulo p para os primeiros 6 números primos p...
  #
  for i to 6 do
    p:=ithprime(i):
    printf("%A %A\n",p,Factor(m) mod p):
  od:
>
>
```

Corpos finitos

```
> restart:
> # Dois polinómios primo em Z_2[X]...
  Factor(x^4+x+1) mod 2;
  Factor(x^4+x^3+x^2+x+1) mod 2;
> # "Dois" F_16...
  alias(alpha=RootOf(x^4+x+1)):
  alias(beta=RootOf(x^4+x^3+x^2+x+1)):

> # Cálculos nos "dois" F_16...
  evala(alpha^4+alpha+1) mod 2;
  evala(alpha^6) mod 2;
  evala(beta^4+beta+1) mod 2;
  gamma1:=beta^3+beta;
  evala(gamma1^4+gamma1+1) mod 2;

> restart:
> # O polinómio primo usado no AES...
```

```
   m:=x^8+x^4+x^3+x+1:
   Factor(m) mod 2;
> alias(alpha=RootOf(m));
> evala((alpha^7+alpha^5+alpha^3+alpha^2+1)*(alpha^6+alpha^5+
  alpha^2+alpha)) mod 2;
> convert(convert(01001101,decimal,binary),hexadecimal);
>
>
```