


```
[ > protect('a_publ');
```

- Funzione di cifratura

```
[ > Cifra := (x, a) -> linalg[dotprod](x, a);  
Cifra := linalg_dotprod
```

- Funzione di decifratura

```
[ > Decifra := proc(C, N, W, M, A)  
  local C1, X, i;  
  X := vector(N);  
  for i from 1 to N do X[i] := 0; od;  
  C1 := (C*W) mod M;  
  for i from N to 1 by -1 do  
    if A[i]<=C1 then  
      X[i] := 1;  
      C1 := C1 - A[i];  
    fi;  
  od;  
  RETURN(evalm(X));  
end;  
Decifra := proc(C, N, W, M, A)  
local C1, X, i;  
X := vector(N);  
for i to N do X[i] := 0 end do;  
C1 := C*W mod M;  
for i from N by -1 to 1 do if A[i] ≤ C1 then X[i] := 1; C1 := C1 - A[i] end if  
end do;  
RETURN(evalm(X))  
end proc
```

- Esempio

```
[ Il messaggio  
[ > x := [0,0,1,0,1,0,1,0,1,1];  
x := [0, 0, 1, 0, 1, 0, 1, 0, 1, 1]  
[ La cifratura  
[ > C := Cifra(x,a_publ);  
C := 607763  
[ La decifratura  
[ > Decifra(C,n,inv_w,m,a_priv);  
[0, 0, 1, 0, 1, 0, 1, 0, 1, 1]
```