CRYPTOGRAPHIE À BASE DE SAC À DOS

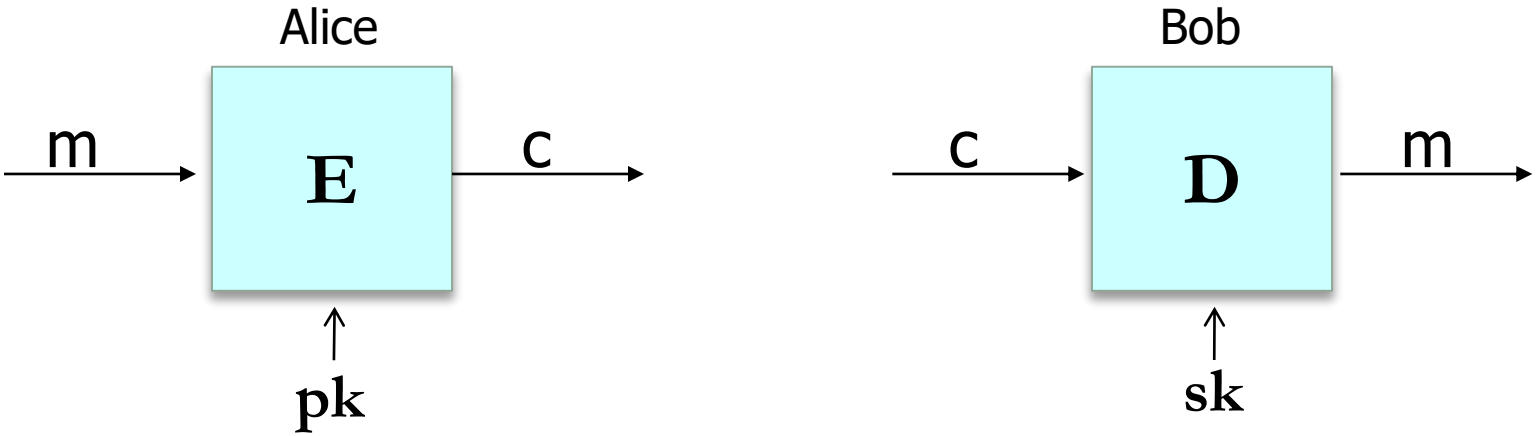
Réalisé par:
Loubna EL BACHIRI
Tarik RAHMATALLAH

Jugé par:
Mme. Hanane El Bakkali
Mr. Hussain BENAZZA

1. Cryptographie publique
2. Problème général de sac à dos
3. Cryptosystème de Merkle-Hellman
4. Réduction de réseau
5. Cryptanalyse du système de Merkle-Hellman
6. Cryptosystème de Chor-Rivest

CRYPTOGRAPHIE PUBLIQUE

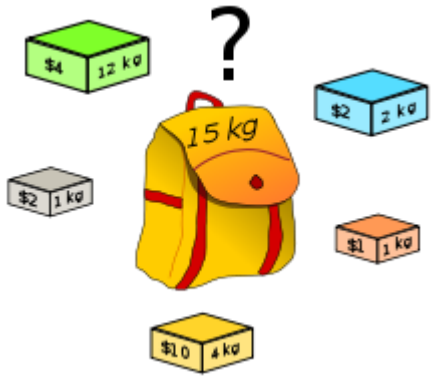
Bob génère une paire de clés(PK, SK) et donne PK à Alice



PROBLÈME DE SAC À DOS

PROBLÈME GÉNÉRAL DE SAC À DOS

Comment remplir le sac de façon à maximiser la valeur totale des objets tout en respectant la capacité du sac ?



Problème NP-complet !

CRYPTOSYSTÈME DE MERKLE ET HELLMAN

- Défini par Merkle et Hellman en 1978.
- Cryptosystème asymétrique.
- Basé sur le problème de la somme des sous ensembles.

CRYPTOSYSTÈME DE MERKLE ET HELLMAN

Génération de clés

- Choisir un entier n suffisamment grand (taille du bloc)
- Choisir une suite (a1, a2,…., an) super croissante.
- Choisir un entier N supérieur à la somme des bi
- Choisir un entier A inférieur à N et premier avec N
- Calculer les ai = A^{-1}*bi mod M, les trier en ordre croissant et garder la permutation.

La clé publique est la suite des bi tandis que la clé privée est composée de N, A et (a1, …., an)

CRYPTOSYSTÈME DE MERKLE ET HELLMAN

Chiffrement

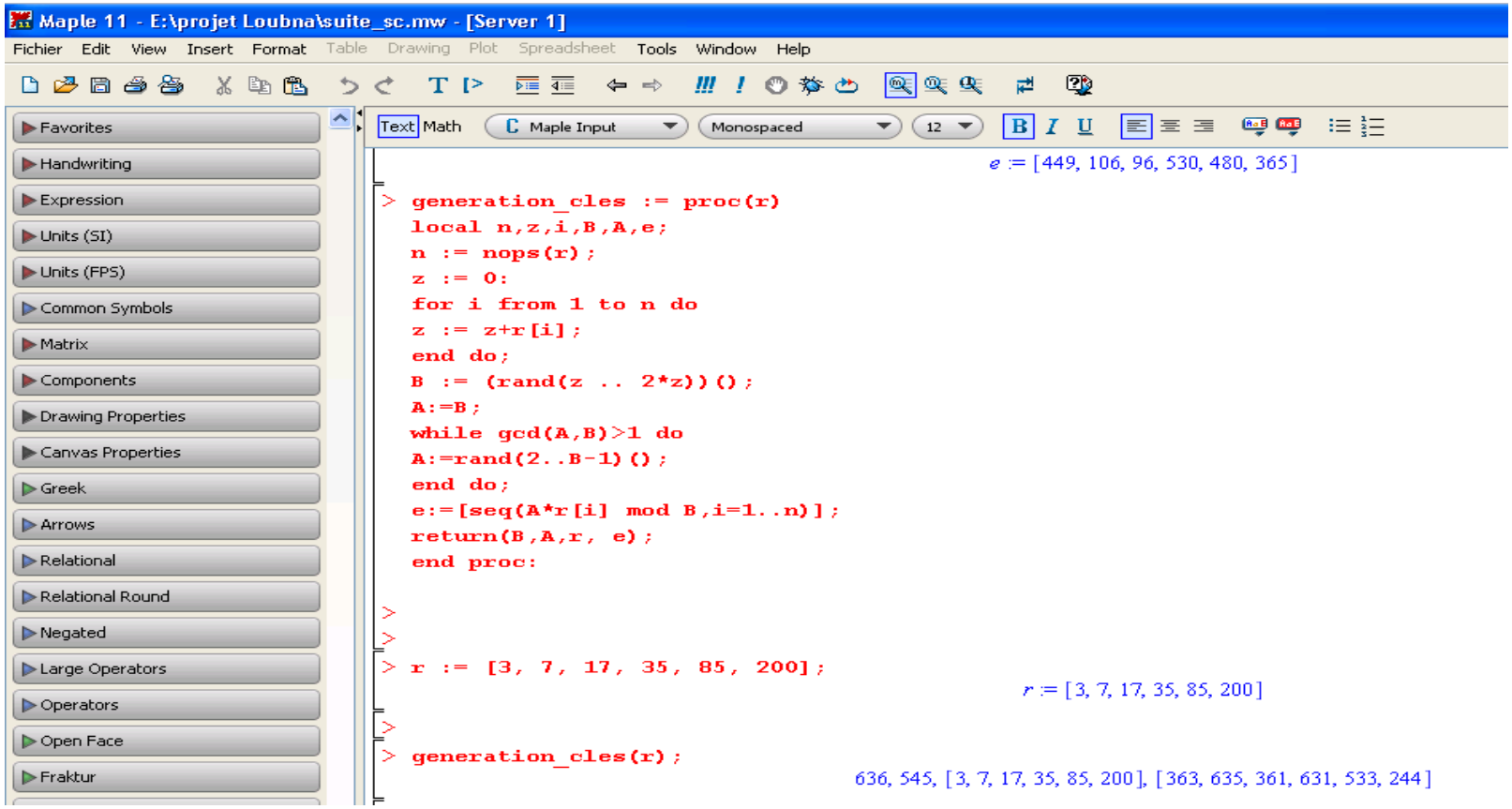
- Le message chiffré est écrit en binaire sous la forme m1,m2…mn avec mi = 0 ou 1.
- On calcule le chiffré d'un message comme suit : c=∑mi*bi

Déchiffrement

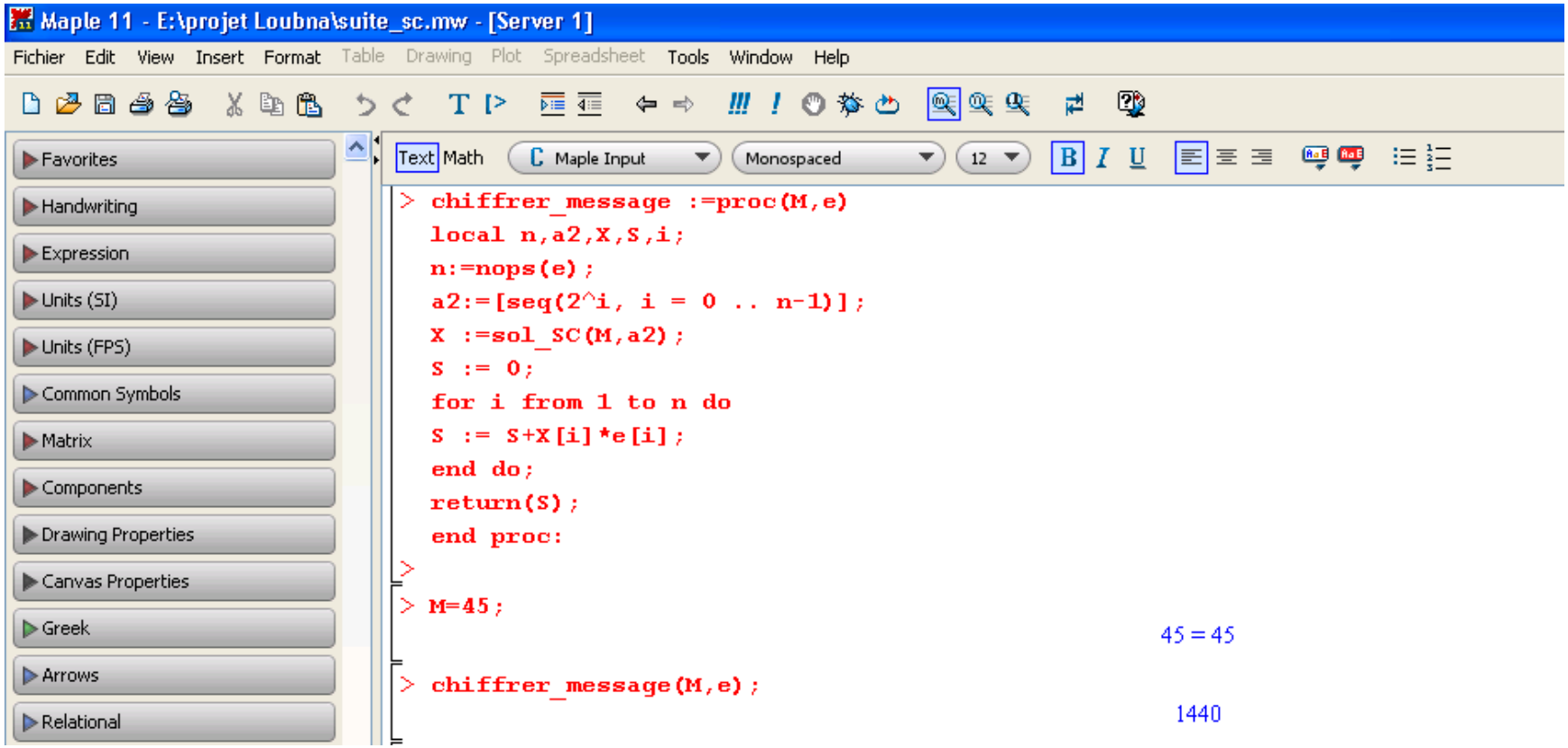
- Calculer d= $A^{-1} \times c \bmod N$.
- Puis calculer les e1, e2, …., en tels que d=∑ei*ai. Il s'agit en fait de résoudre un problème de sac à dos très simple (suite super croissante)

  Ei=Mi pour tout i

IMPLÉMENTATION SOUS MAPLE



IMPLÉMENTATION SOUS MAPLE



IMPLÉMENTATION SOUS MAPLE


```
> dechiffrer_cryptogramme := proc(S,A,B,a)
  local S1,X1,M,i;
  S1:=(S*modp(1/A, B)) mod B;
  X1 := sol_SC(S2,a);
  M := 0:
  for i from 0 to n-1 do
  M := M+X1[i+1]*2^i
  end do:
  return(M);
  end proc:

> dechiffrer_cryptogramme(S,A,B,a);
```

45

CRYPTANALYSE DU SYSTÈME DE MERKLE-HELLMAN

RÉDUCTION DE RÉSEAU

- Soit B = (b1,…, bn) une famille de vecteurs linéairement indépendants de Rn. Le réseau engendré par la base B est l'ensemble :

$$L(B) = \{ \sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z} \}$$

- L'idée de la réduction de réseau est de calculer une nouvelle base engendrant le même réseau que (b1,...,bn) mais dont les vecteurs sont plus courts et plus orthogonaux.
- Une base (b1, b2,..., bn) est LLL-réduite si, la base (b1*, b2*,..., bn*) produite par la méthode d'orthogonalisation de Gram-Schmidt vérifie :

$$|\mu_{i,j}| \leq 1/2 \quad \text{pour} \quad 1 \leq j < i \leq n \qquad (1)$$

$$3/4 \, ||b_{i-1}^*||^2 \leq ||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2 \quad \text{pour } 1 < i \leq n \qquad (2)$$

CRYPTANALYSE DU SYSTÈME DE MERKLE ET HELLMAN

- Attaquer le cryptosystème de Merkle et Hellman revient a résoudre l'équation: $\sum_{i=1}^{n} mi*ai=c$

- On considère le réseau engendré par les lignes de la matrice suivante :

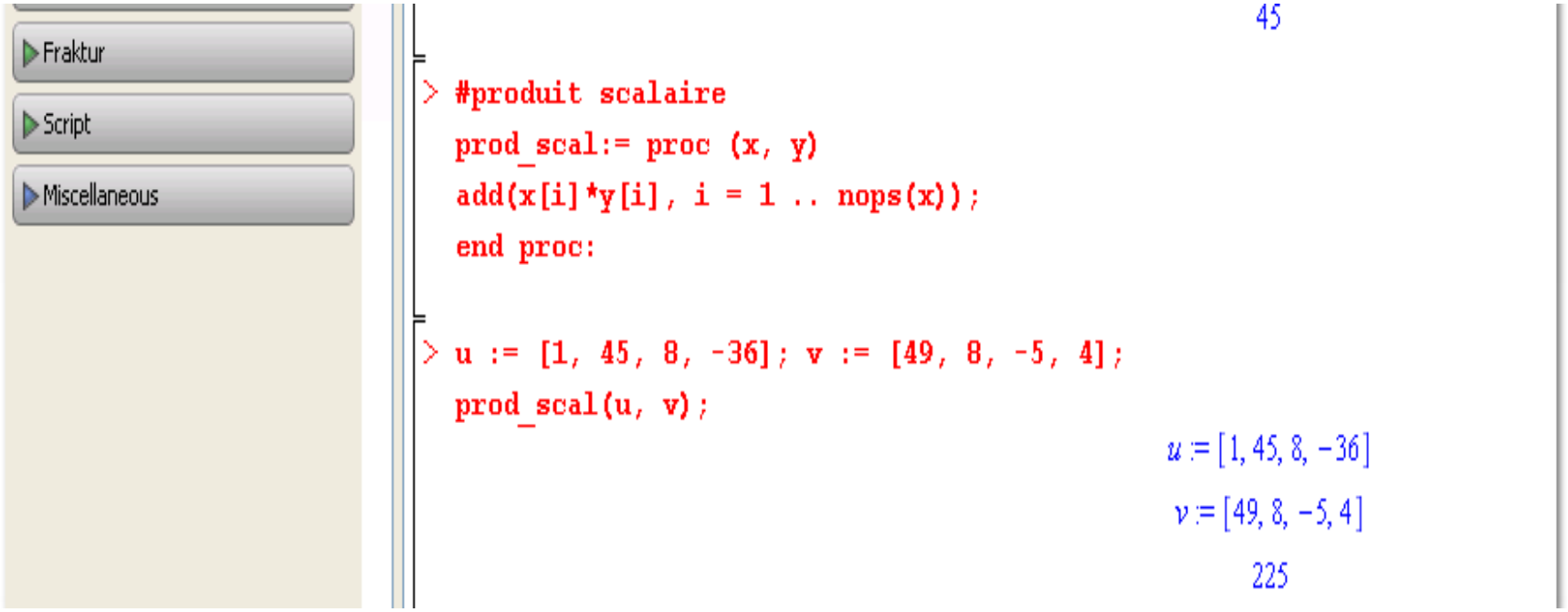
$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & a_1 \\ 0 & 1 & 0 & \dots & 0 & a_2 \\ 0 & 0 & 1 & \dots & 0 & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & a_n \\ 0 & 0 & 0 & \dots & 0 & c \end{pmatrix}$$

CRYPTANALYSE DU SYSTÈME DE MERKLE ET HELLMAN

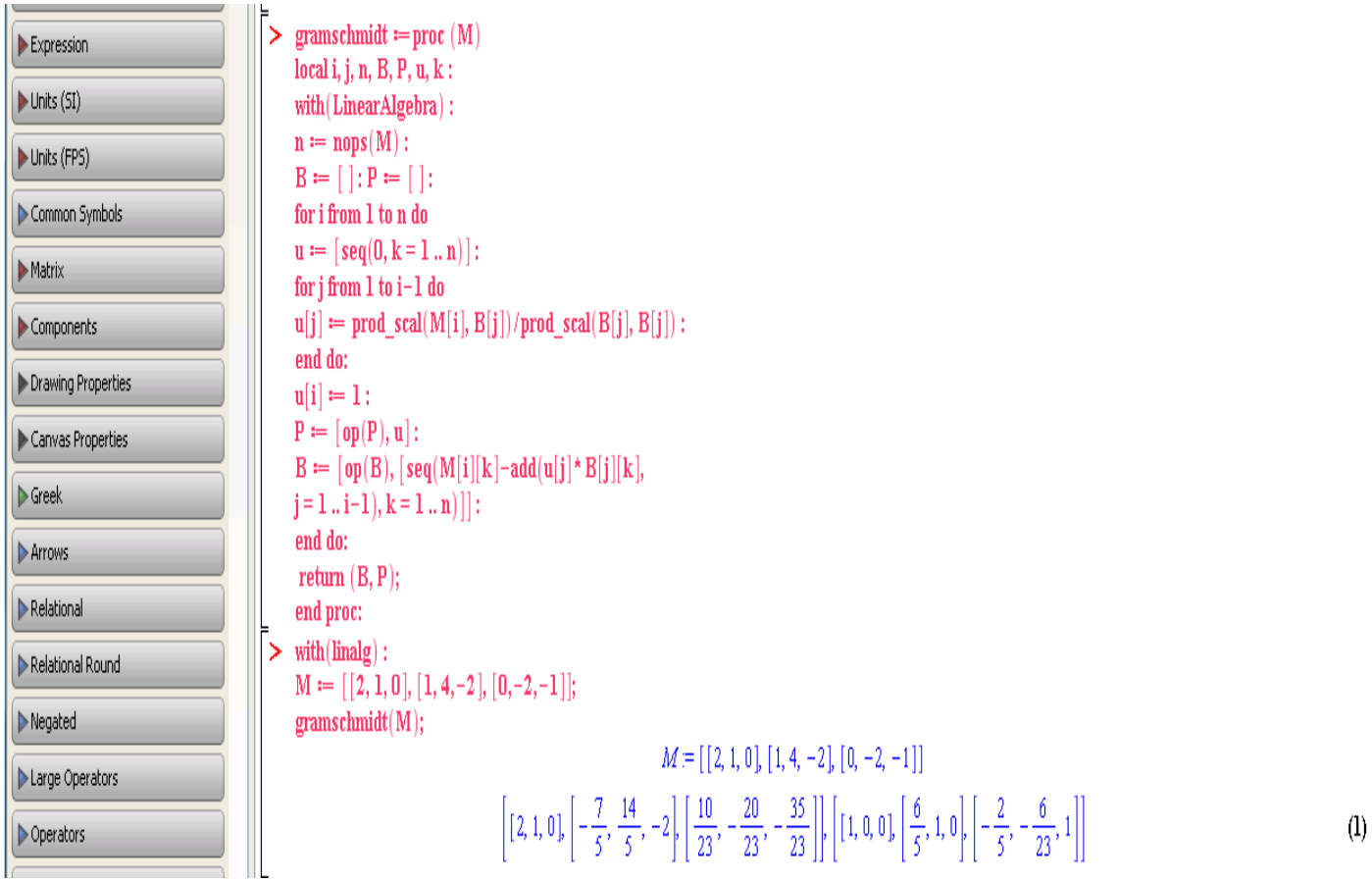
Le plus court vecteur doit vérifier les conditions suivantes:

- $| m_{n+1} | = 0$
- $| m_i | \leq 1$ pour $1 \leq i \leq n$
- $\sum_{i=1}^{n} m_i * a_i = c$

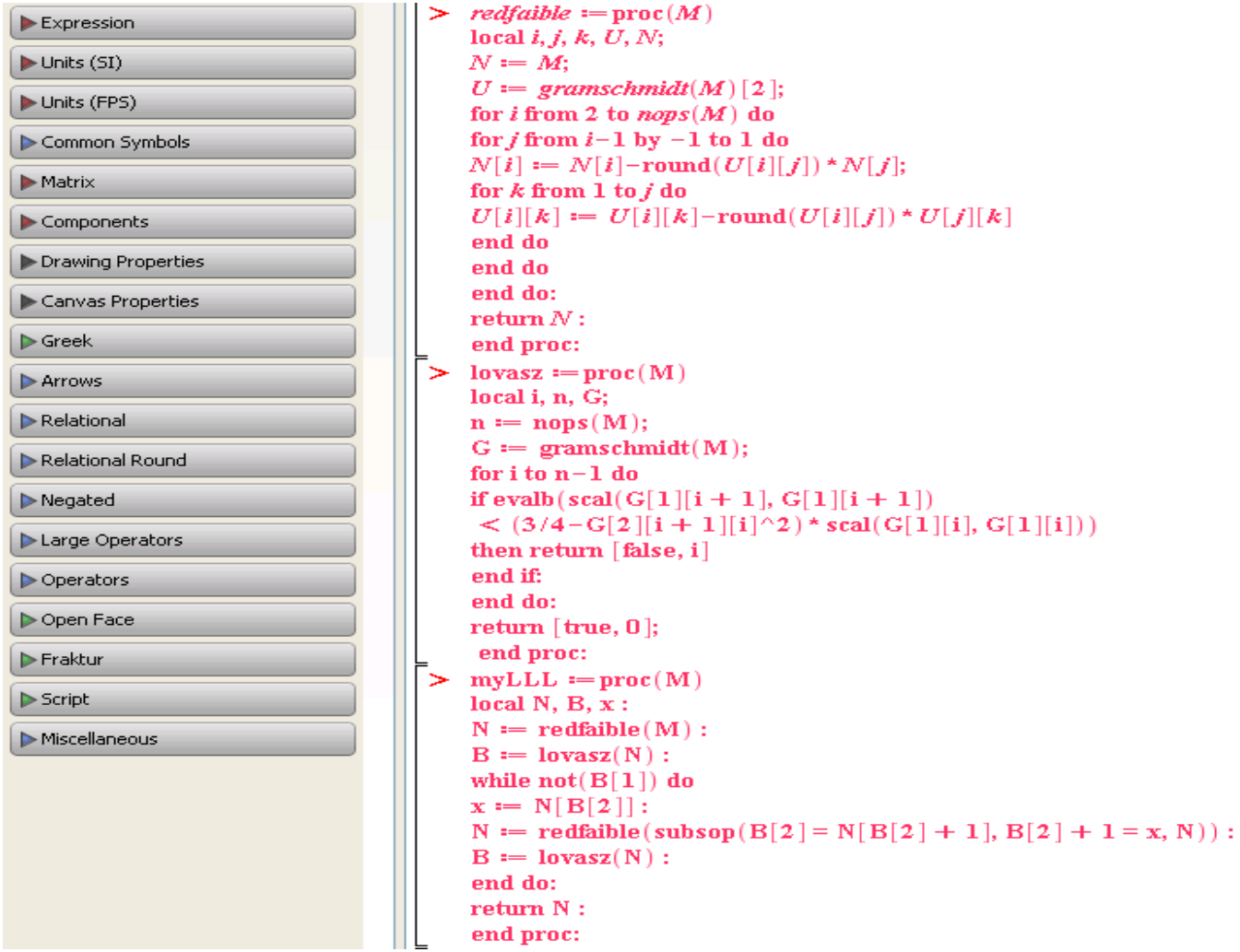
IMPLÉMENTATION SOUS MAPLE



IMPLÉMENTATION SOUS MAPLE



IMPLÉMENTATION SOUS MAPLE



CRYPTOSYSTÈME DE CHOR-RIVEST

Génération de clés

- ✓ choisir un nombre premier P et un nombre entier h , et créer un corps fini GF(P^h) = Zp[x]/f(x) où f(x) est un polynôme de degré h qui est irréductible dans Z/pZ .soit g(x) un élément primitif de Z/pZ.

- ✓ Pour chaque i ϵ Z/pZ calculer les logarithmes discrets ai = $\log_{g(x)}(x+i)$.

- ✓ Choisir un entier aléatoire d avec $0 \leq d \leq P^h - 2$.

- ✓ Calculer ci = (ai+d) mod P^h-1 pour $0 \leq i \leq p-1$.

- ✓ la clé publique est([c0,c1,……..cp-1],P,h) et la clé privée est [f(x),g(x),d].

CRYPTOSYSTÈME DE CHOR-RIVEST

chiffrement

- Les messages sont des suites binaires de longueur P avec exactement h 1

$(\sum_{i=0}^{p-1} \mathrm{mi} = h)$.

- Le cryptogramme est obtenu par :

C= $\sum_{i=0}^{p-1} mici(mod\ P^h - 1)$.

déchiffrement

- Calculer r = (C–hd) mod (P^h-1).
- Calculer u(x) = $g(x)^r$ (mod f(x)).
- Calculer s(x) = u(x) + f(x) .
- Factoriser s(x) en facteurs linéaires S(x) = $\prod_{j=1}^{h}(x + tj)$

CONCLUSION

- après la parution de la méthode de Merkle-Hellman, il a été remarqué que des répétitions pouvaient apparaître.

- L'algorithme LLL permet de déchiffrer quasi systématiquement le message codé.

- la méthode de Chor-Rivest ne semble pas encore avoir été attaquée.

- non plus utilisée car pour avoir une résistance comparable à du RSA 512 bits, il faudrait une clé publique de l'ordre de 36000 bits.

Merci pour votre attention

CRYPTOGRAPHIE À BASE DE SAC À DOS

Réalisé par:
Loubna EL BACHIRI
Tarik RAHMATALLAH

Jugé par:
Mme. Hanane El Bakkali
Mr. Hussain BENAZZA