Un exemple de chiffrement à clé publique: le codage . . « quadratique »

Activité proposée par Pierre Mari, Professeur de Mathématiques, Sujet «unplugged» (sans ordinateur)

Imaginons qu'Alice souhaite recevoir un message chiffré de Bob. sans lui donner la clé qui lui permettra de déchiffrer le message (de peur que cette clé ne soit interceptée par une personne malveillante) ; elle va donc produire deux clés :

- Une clé publique (publique signifie qu'elle peut être connue de tous sans danger)
- Une clé secrète (qu'Alice va conserver précieusement)

La transmission du message se fait alors de la manière suivante :

- Alice transmet à Bob la clé publique.
- Bob chiffre son message à l'aide de la clé publique.
- Il envoie le message chiffré à Alice.
- Alice déchiffre le message de Bob en utilisant sa clé secrète.

Un tel système, appelé aussi chiffrement asymétrique, a été imaginé à la fin des années soixante dix ; le plus connu est le système RSA utilisé aujourd'hui dans une multitude d'applications, notamment les transactions sécurisées via internet. L'objectif de cette activité est la mise en œuvre d'un chiffrement à clé publique.

1ère partie : un peu de math pour commencer.

On considère deux nombres **positifs** a et b et pose $S=a+b$ et $P=ab$ et on considère la fonction f définie pour tout nombre x par $f(x)=x^2+Sx+P$.

1/ Vérifier que pour tout nombre x on a $f(x)=(x+a)(x+b)$.

2/ Prendre pour a et b deux valeurs particulières et tracer l'allure de la courbe représentative de f ; quel est le sens de variation de f sur l'intervalle $[0;+\infty[$?

3/ Un défit : peut-on trouver deux entiers positifs dont la différence égale 3 et le produit égale 180 ?

2ème partie : **description du système de chiffrement.**

1/ Alice doit recevoir un message de Bob : pour simplifier on considère que ce message est un nombre positif **m.** Alice choisit deux nombres entiers positifs a et b : le couple $(a;b)$ constitue la clé secrète qu'elle conserve précieusement.

- Alice calcule $S=a+b$ et $P=ab$: le couple $(S;P)$ constitue la clé publique.
- Alice transmet la clé publique à Bob.
- Bob calcule $m'=m^2+Sm+P$
- Bob transmet la valeur trouvée m' à Alice.
- Alice cherche la solution positive de l'équation $(x+a)(x+b)=m'$ en écrivant m' de toutes les manières possibles comme produit de deux facteurs : la valeur trouvée de x est m .

Exemple : Alice choisit $a=8$ et $b=3$: sa clé privée est $(8;3)$; elle transmet la clé $(11;24)$ à Bob ; Bob veut transmettre à Alice le message $m=4$; grâce à la clé publique, il calcule $4^2+11\times4+24=84$ et le transmet à Alice ; Alice pose l'équation (x+3)(x+8)=84 ; pour retrouver la valeur de x , Alice remarque que $84=7\times12$ et elle en déduit que la solution positive de l'équation est $x=4$. Elle sait que le message envoyé par Bob est $m=4$.

2/ Supposons qu'Alice choisisse la clé privée $(a;b)=(2;8)$

- Quelle est la clé publique qu'elle envoie à Bob ?
- Bob souhaite chiffrer le message clair $m=3$; quel message va-t-il transmettre à Alice ?
- Comment Alice va-t-elle déchiffrer le message ?

3/ Supposons qu'Alice choisisse la clé privée $(a;b)=(5;7)$; elle calcule la clé publique correspondante, la

transmet à Bob qui lui renvoie le message chiffré $m'=120$; quel est le message clair ?

3ième partie : à vous de jouer

Travail à faire par binôme :

- L'un des membres du binôme joue le rôle d'Alice : il choisit une clé (simple pour éviter des calculs trop compliqués) ; il la transmet à l'autre membre qui joue le rôle de Bob.
- Bob choisit un message m (simple), le chiffre avec sa clé privée et le transmet à Alice.
- Alice déchiffre le message grâce à publique.

Échanger ensuite les rôles de Bob et d'Alice et faire un compte-rendu écrit de vos transmissions.