Cryptographie : Protocole de Shamir

Toutes les coordonnées sont données dans un repère orthonormé.

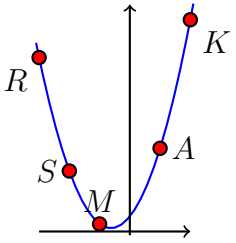
Question 1 (Interpolation polynômiale)**.**

(a) Soient trois points $(-3;23)$, $(2;28)$, $(-1;1)$. Montrer que le polynôme du second degré $f : x \mapsto 4x^2 + 5x + 2$ passe par ces trois points.

(b) Soient deux points $(2;28)$ et $(-1;1)$. Trouver au moins deux polynômes du second degré dont la représentation graphique passe par ces points. Quelle est alors la valeur de l'ordonnée à l'origine dans chaque cas ?

Bilan On admet la propriété suivante : Par deux points d'abscisses différentes passe une infinité de polynômes du seconde degré ; par trois points d'abscisses différentes passe un et un seul polynôme du second degré.

Question 2 (Application pratique)**.** Cinq bandits Robin, Samah, Margot, Alex et Killian ont caché leur butin dans un coffre fermé par un code composé de chiffres. Ils se font confiance, mais il se disent que si l'un d'entre eux est capturé par la police, il finira, sous la pression, par donner le code aux autorités. Pour se protéger de cette situation, ils se partagent le secret en utilisant le protocole de partage de clef secréte de Shamir (*Shamir's Scharing Secret Scheme* (ou SSSS) en anglais). Ils décident d'un code pour le coffre. Ils considèrent ensuite le polynôme $ax^2 + bx + c$ (où a et b sont deux nombres entiers quelconques, non nuls, et c est le code du coffre), et chacun se voit attribuer un point sur la courbe de ce polynôme, connu de lui seul.



(a) Pour préparer un nouveau larcin, Robin, Killian et Margot veulent ouvrir le coffre y prendre du matériel. Retrouver le code du coffre à partir de leurs points respectifs $R(-3;23)$, $K(2;28)$, $M(-1;1)$.

(b) Leur larcin ne s'est pas passé comme prévu, et Killian et Margot ont été pris. Ils finissent par donner leurs points $K(2;28)$ et

$M(-1;1)$ à la police. Montrer qu'à partir de ces seules informations, la police ne peut pas retrouver le trinôme original, et donc le code du coffre.