De nombreux bons livres, sur la cryptographie sont disponibles et en particulier sur la cryptographie elliptique. La rubrique "bibliographie" de ce site en donne un échantillon. Cependant je voudrais faire une mention spéciale pour le livre

Courbes elliptiques *- Une présentation élémentaire pour la cryptographie*

de Philippe Guillot, aux éditions Hermes-Lavoisier (2010). En effet ce livre donne un remarquable exposé de la question. Tout l'aspect "géométrie algébrique" des courbes elliptiques sur les corps finis, indispensable au cryptographe, est repris dans le cadre strict des courbes elliptiques. Tout est entièrement démontré de manière rigoureuse et élémentaire. Mais attention, élémentaire ne veut pas dire superficiel. Les questions abordées sont loins d'être simples : par exemple les morphismes sont étudiés avec leurs propriétés liées aux ramifications, on étudie aussi les points de torsion, les accouplements de Weil et plein d'autres choses à la fois passionnantes et utiles. Le problème du logarithme discret sur les courbes elliptiques est mis en perspective dans un chapitre général intitulé "Le problème du logarithme discret" qui donne un panorama très complet. C'est à mon avis un livre qui manquait, entre les exposés plutôt descriptifs et ceux qui font reposer l'étude des courbes elliptiques sur des résultats généraux de géométrie algébrique et qui sont d'un abord plus difficile. En outre l'auteur nous propose une liste d'exercices corrigés,

On peut trouver des détails sur la page consacrée à ce livre du site de l'éditeur Lavoisier.