Exercice 3 Signatures RSA et fonctions de hachage cryptographiques (7 points)

3.1 Rappeler le schéma de signatures RSA « naïf » vu en cours.

3.2 Montrer qu'en multipliant deux signatures valides s_1 et s_2 sur des messages m_1 et m_2 on obtient une signature s' valide pour le message $m' = m_1 \cdot m_2$. Comment est-ce qu'on appelle cette propriété ?

3.3 Pourquoi cette propriété est-elle embêtante d'un point de vue de sécurité ?

Afin d'améliorer ce schéma de signature, considérons maintenant un schéma où on signe le haché $h(m)$ plutôt que le message m lui-même.

3.4 Rappeler les trois propriétés de sécurité d'une fonction de hachage cryptographique.

3.5 Laquelle des trois propriétés des fonctions de hachage garantit la sécurité de la signature ici ? Expliquer pourquoi.

3.6 Quelles sont les avantages de ce schéma, par rapport au schéma initial, en matière de sécurité et d'efficacité ?

Exercice 4 Cryptographie asymétrique : ElGamal (4 points)

Considérons le système de chiffrement ElGamal, en utilisant le groupe multiplicatif des entiers modulo $p = 19$, et le générateur $g = 2$.

4.1 Alice choisit sa clé sécrète $s = 11$. Calculer sa clé publique h.

4.2 Bob souhaite envoyer le message $m = 7$ à Alice. Calculer le chiffré de m, en utilisant la valeur aléatoire $r = 3$.

4.3 Montrer que Alice obtient bien m quand elle déchiffre.

Considérons maintenant la clé publique de Bob $h' = 18$.

4.4 Pouvez-vous retrouver sa clé sécrète s' associé ? Comment ? Quelle erreur Alice et Bob ont-ils commis quand ils ont mis en place leur système de chiffrement ?