IFT3275 - Examen Final

Arnaud L'Heureux

22 avril 2021

Remise: 23 avril, 18h00. Les examens remis en retard seront exclus.
Doit obligatoirement être fait individuellement en LaTeX.

1. Démontrez la propriété mutliplicative de RSA: $x_1^e \cdot x_2^e \equiv (x_1 \cdot x_2)^e \pmod{n}$. RAPPEL: un exemple n'est pas une preuve.

2. Considérez un échange de clef Diffie-Hellman effectué grâce à un corps de galois $GF(2^m)$. L'arithmétique est effectué dans $GF(2^5)$ à l'aide du polynôme irréductible $P(x) = x^5 + x^2 + 1$. L'élément primitif est le suivant: $\alpha = x^2$. Les clefs privées sont $a = 3$ et $b = 12$. Quelle est la clef établie k_{AB}?

3. Pour les fonctions de hachage cryptographiques, il est important d'utiliser une largeur de fonction assez grande telle que 160 bits pour résister aux attaques basées sur le "birthday paradox". Pourquoi est-ce qu'un taille de sortie beaucoup plus petite (telle que 60 bits) est suffisante dans le cas des MACs? Pensez à ce qu'Oscar doit faire s'il voit passer un message clair x et $MAC_k(x)$ entre Alice et Bob.

4. Dérivez les formules introduites en classe pour additionner deux points sur les courbes elliptiques (comment déterminer $R = (x_3, y_3)$ à partir des coordonnées de P et Q). INDICE: Trouvez l'équation d'une droite à travers P et Q. Insérez-la dans l'équation de la courbe elliptique. Vous devrez éventuellement trouver les racines du polynôme $x^3 + a_2x^2 + a_1x + a_0$. En dénotant ces trois racines comme étant $r_0,\ r_1,\ r_2$, vous pouvez utiliser le fait que $r_0 + r_1 + r_2 = -a_2$.

5. Soit la courbe elliptique $E : y^2 \equiv x^3 + 2x + 2 \mod 17$. Pourquoi est-ce que tous les points sur cette courbes sont des éléments générateurs?