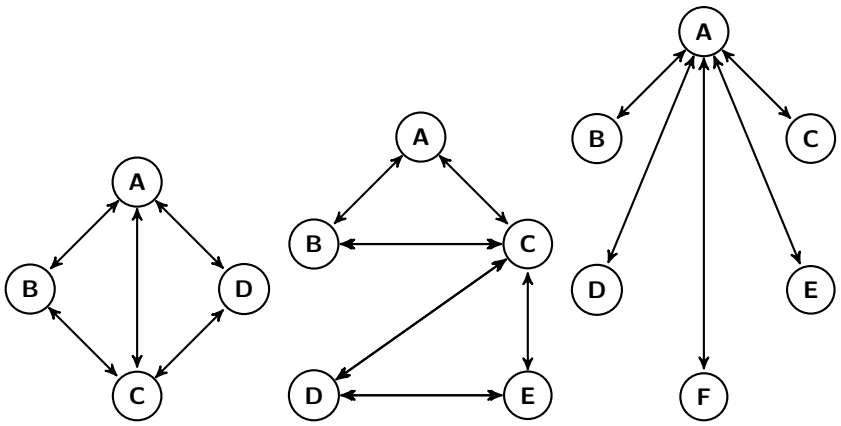
D31: Protocoles cryptographiques
TD 1: Cryptographie à clé publique

Exercice 1. Questions en vrac

1. Quelle est la différence entre cryptographie à clé publique et cryptographie à clé privée?
2. Les fonctions de chiffrements des systèmes à clé publique sont bien plus lentes que leurs homologues des systèmes à clé privée (le chiffrmeent AES-128 est 20 fois plus rapide que celui de RSA-1024 par exemple). Comment pallie-t-on se problème en pratique?
3. Pour chacun des réseaux suivants, dire combien il faut de de clés dans le cadre de d'un système à clé publique ou à clé privée.



(a) (b) (c)

4. On considère les deux fonctions de chiffrement/déchiffrement d'un système à clé publique $D(K_{sec}, .), E(K_{pub}, .)$. On suppose le système sûr. On propose de chiffrer un message long $M = m_1 \dots m_n$ (où les m_i sont des caractères) de la façon suivante:

$$e(M) = E(K_{pub}, m_1) \dots E(K_{pub}, m_n).$$

Ce chiffrement est-il sûr? Expliquer.

Exercice 2. Cryptosystème Merkle-Hellman

1. On considère un système de Merkle-Hellman avec les paramètres

$$K_{pub} = (\{2130, 4260, 2110, 3774, 2822, 3314, 1436, 4273\})$$

et

$$K_{sec} = (\{5, 10, 28, 78, 191, 607, 1294, 2695\}, 426, 4909)\,.$$

   1. Chiffrer le message 01010111.
   2. Déchiffrer le message 13458.

On considère maintenant un système de MH quelconque, la clé publique est un ensemble de n entiers.

$$K_{pub} = (\{b_1, \ldots, b_n\}) \text{ et } K_{sec} = (\{a_1, \ldots, a_n\}, q, p)\,.$$

2. Montrer que ce système est vulnérable à une attaque à chiffrés choisis (tip: il faudra demander à l'oracle de déchiffrer n chiffrés).
3. Montrer qu'il suffit de trouver deux entiers q' et p' (pas forcément q et p) tels que la suite $(b_i {q'}^{-1} \mod p')_i$ soit supercroissante pour casser le système.
4. Montrer que la connaissance de l'entier p et de n'importe quel a_i suffit à casser le système.