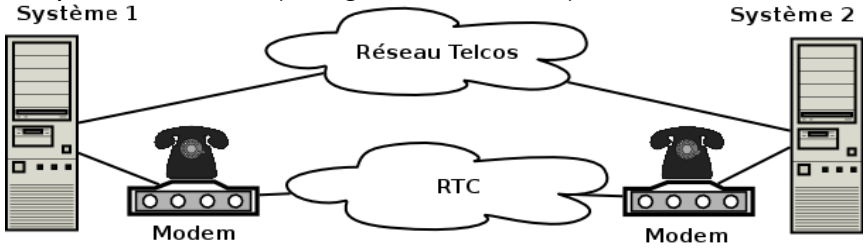
TD/TP n°2 : Sûreté des fonctionnements et cryptographie appliquée aux échanges

Exercice : **MTTR/MTBF**

Soient deux systèmes informatiques identiques interconnectés via les services d'un opérateur et une liaison téléphonique de secours (cf. figure ci-dessous).



Quel est, pour l'ensemble du système, la disponibilité, l'indisponibilité et la MTBF du système, compte tenu des éléments du tableau ci-dessous ? Par hypothèse, on admettra que la MTBF de l'opérateur inclut la liaison d'abonné et les modems d'extrémité.

	MTBF	*MTTR*
Système 1	4 mois	8 heures
Système 2	4 mois	8 heures
Modem	2 ans	5 heures
RTC	2 ans	24 heures
Telcos	2 ans	2 heures

On considérera qu'un mois représente 200 heures et une année 2400 heures.

Exercice : **Chiffrement symétrique et asymétrique**

Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre.

Le groupe décide d'utiliser un système symétrique de chiffrement.

1. Quel est le nombre minimal de clefs symétriques nécessaires ?
2. Donner le nom d'un algorithme de chiffrement symétrique reconnu.

Le groupe décide ensuite de remplacer ce système par un système asymétrique.

1. Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées ?
2. Alice souhaite envoyer des informations chiffrées et signées à Bob (Alice et Bob appartiennent tous les deux au groupe). Quelle(s) clef(s) Bob doit-il utiliser ?
3. Donner le nom d'un algorithme de chiffrement asymétrique reconnu.

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (i.e. qui utilise à la fois le cryptographie symétrique et asymétrique)

1. Donner les raisons qui ont poussées le groupe à utiliser un tel système.

Exercice : **Algorithme RSA**

Le premier algorithme de chiffrement asymétrique et de signature proposé, l'algorithme RSA, a été publié en 1978 par Rivest, Shamir et Adleman. Sa sécurité repose sur la difficulté de factoriser un entier (et plus spécifiquement du problème de l'extraction de racines modulaires).

En particulier, il est difficile de retrouver clair à partir de chiffré, de cléChiffre de n et de l'algorithme de chiffrement suivant $chiffré = (clair)^{cléChiffre} \text{ modulo } (n)$

Avec n, produit de 2 nombres premiers p et q, et cléChiffre, premier avec ((p-1) (q-1))

Par contre si on connaît p et q, alors il est possible de calculer cléDéchiffre à partir de

cléDéchiffre = (1 modulo ((p-1) (q-1))) / cléChiffre

On définit alors une fonction de chiffrement $x \rightarrow x^e \bmod n$, et une fonction de déchiffrement $x \rightarrow x^d \bmod n$ ainsi qu'une clé publique (e,n) et une clé privée (d,n).

L'algorithme RSA peut être utilisée pour assurer la confidentialité des messages que leur authenticité, c'est-à-dire les signer.

1. En admettant que $x^{ed} = x \bmod n$, montrer que la fonction de chiffrement proposée est bien l'inverse de la fonction de déchiffrement.
2. Détailler la procédure à suivre pour générer un couple (clé publique, clé privée)
3. Chiffrer le message « 21 » avec la clé publique (103, 143). Le calcul peut être facilement fait à la main en remarquant que $21^4 = 1 \bmod (143)$
4. Sachant que n = 11 * 13, calculer la clé privée associée à la clé publique (103, 143)
5. Déchiffrer le message obtenu à la question 3 afin de trouver le message clair

Exercice : **Certificats**

Discuter les trois scénarii suivants en termes de sécurité :

1. Deux certificats différents sont signés par la même clé privée
2. Deux certificats différents contiennent la même clé publique
3. Deux certificats différents ont la même empreinte