

---

## Cryptographie à clé publique – Feuille de TD 6

11/03/2026

---

Le corrigé de certains exercices sera disponible à l'adresse suivante :

<https://lvz1.fr/teaching/2025-26/cp.html>

(★) exercice fondamental    (★★) pour s'entraîner    (★★★) pour aller plus loin     sur machine

---

### Exercice 1. (★) Un nouveau protocole d'identification ?.

Alice souhaite s'identifier auprès de Bob. On suppose qu'Alice et Bob détiennent un secret commun  $x \in \{0,1\}^t$ , pour  $t \geq 1$ , qui doit servir à plusieurs identifications. Le protocole suivant est proposé :

1. Bob choisit une chaîne aléatoire  $r \in \{0,1\}^t$  et l'envoie à Alice
2. Alice calcule  $y = r \oplus x$  et renvoie  $y$  à Bob.
3. Bob vérifie que  $x = r \oplus y$ .

**Question 1.**– Pourquoi ce protocole ne peut pas être utilisé pour plusieurs identifications ?

**Question 2.**– Quelle étape d'un protocole d'identification à trois passes manque-t-il dans ce protocole ?

### Exercice 2. (★★) Schéma d'identification de Feige–Fiat–Shamir.

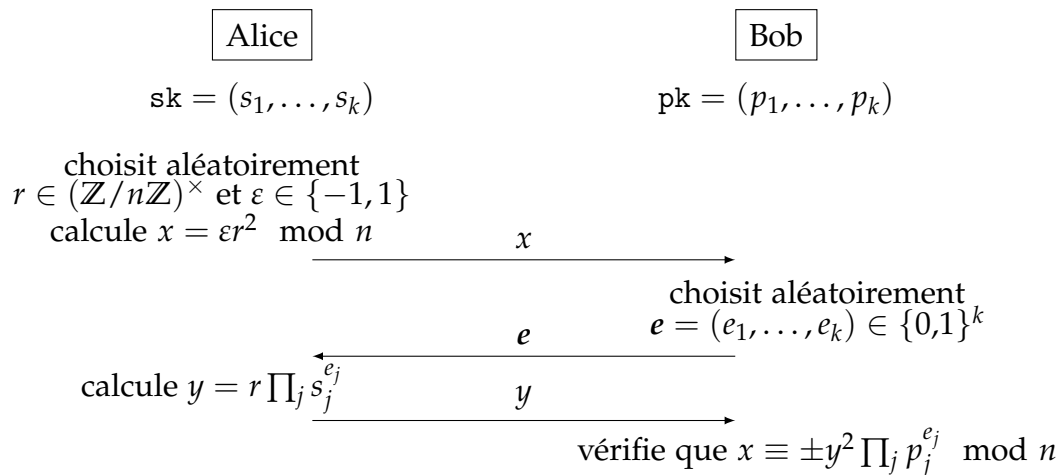
Dans cet exercice, on s'intéresse au schéma d'identification de Feige-Fiat-Shamir.

Dans le réseau de participants, une autorité de confiance choisit secrètement  $p$  et  $q$  deux grands nombres premiers, puis calcule et publie  $n = pq$ . On fixe ensuite  $k$  un entier, typiquement de taille  $\log_2 \log_2 n$ .

Alice, une utilisatrice du réseau, procède comme suit pour engendrer une paire de clefs :

1. Alice choisit aléatoirement  $s_1, \dots, s_k \in (\mathbb{Z}/n\mathbb{Z})^\times$ .
2. Pour tout  $j = 1, \dots, k$ , Alice choisit  $\varepsilon_j \in \{-1, 1\}$  aléatoirement, puis calcule  $p_j = \varepsilon_j / s_j^2$ .
3. La clé publique d'Alice est  $pk = (p_1, \dots, p_k)$ , la clé privée d'Alice est  $sk = (s_1, \dots, s_k)$ .

Le protocole d'identification se déroule ainsi :



**Question 1.**– Démontrer que le protocole d'identification est valide.

**Question 2.**– Démontrer que, si un attaquant connaît le défi  $e$  de Bob **avant** de réaliser son engagement  $x$ , alors il peut monter une imposture. En déduire qu'il existe une attaque sur le système qui réussit avec probabilité  $2^{-k}$ .

**Question 3.**– Selon vous, sur quel problème (difficile) repose la sécurité du schéma? Donner une justification succincte.

Dans les questions suivantes, on cherche à démontrer que le protocole d'identification de Feige-Fiat-Shamir est une **preuve de connaissance à divulgation nulle**. Autrement dit, les itérations du protocole ne révèlent aucune information sur le secret  $sk$  d'Alice.

Pour obtenir cette propriété, l'idée est de démontrer que l'on peut simuler la distribution du transcript  $(x, e, y)$  sans la connaissance de  $sk$ .

**Question 4.**– On suppose que tous les tirages sont uniformes. Quelle loi suit la variable aléatoire  $y$ ?

On définit le **simulateur** de transcript suivant :

1. choisir uniformément  $e' = (e'_1, \dots, e'_k) \in \{0, 1\}^k$ ,
2. choisir uniformément  $r' \in (\mathbb{Z}/n\mathbb{Z})^\times$  et  $\varepsilon' \in \{-1, 1\}$ , puis calculer  $x = \varepsilon' (r')^2 \prod p_j^{e'_j} \pmod n$ ,
3. définir  $y' = r'$ .

**Question 5.**– Démontrer que la loi de  $(x', e', y')$  induite par le simulateur est la même que celle de  $(x, e, y)$  issue du protocole d'identification. En déduire que le protocole est à divulgation nulle.