Chapitre IV
Gestion des Clés Symétriques : Cas de Kerberos

Failles des protocoles

Protocole de Needham et Schroeder

Le système Kerberos

INTRODUCTION

- Un protocole est un algorithme distribué faisant intervenir plusieurs participants
- Chaque participant exécute ses actions sur sa machine
- Un utilisateur peut participer à plusieurs sessions d'un même protocole
- Un utilisateur peut changer de rôle d'une session à une autre
- Tous les utilisateurs légitimes qui y participent se comportent conformément à la spécification du protocole

Capacité de l'intrus

- Peut être un utilisateur régulier
- Peut écouter les messages qui circulent sur le réseau
- Peut éliminer ou modifier les messages qu'il intercepte
- Peut générer des propres messages
- Tous les messages envoyés par l'intrus doivent appartenir à sa base de connaissances
  - Les connaissances initiales + les messages intermédiaires reçus

TERMINOLOGIES

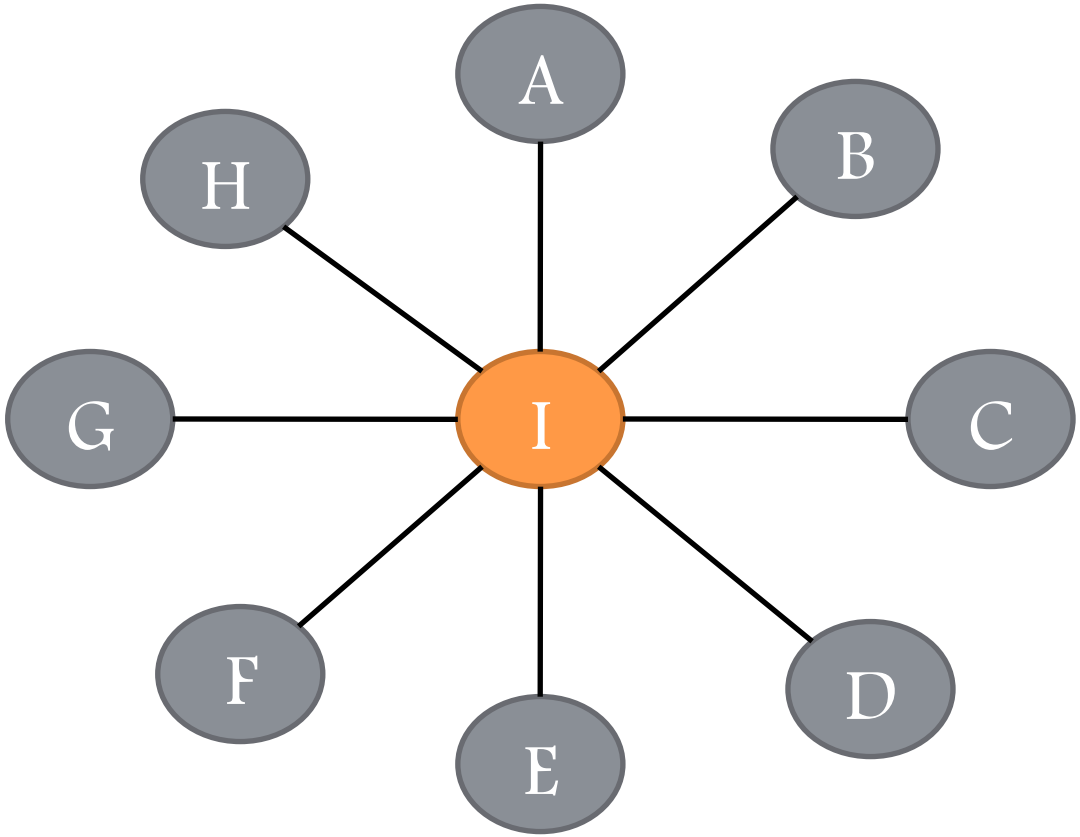
- Nonce ou estampille
  - On note avec Na, un nonce généré par l'utilisateur A
  - Une valeur générée d'une façon aléatoire à chaque session
  - Fraicheur de la session de communication
- Clés de chiffrement
  - Clé symétrique → avec quoi on chiffre et on déchiffre les messages
  - On note avec Kab, une clé symétrique partagée entre A et B
  - On note avec Ka, une clé connue que par A
- Chiffrement
  - On note avec $\{M\}_{Kab}$, un message M chiffré avec une clé Kab

TOPOLOGIE DU RÉSEAU

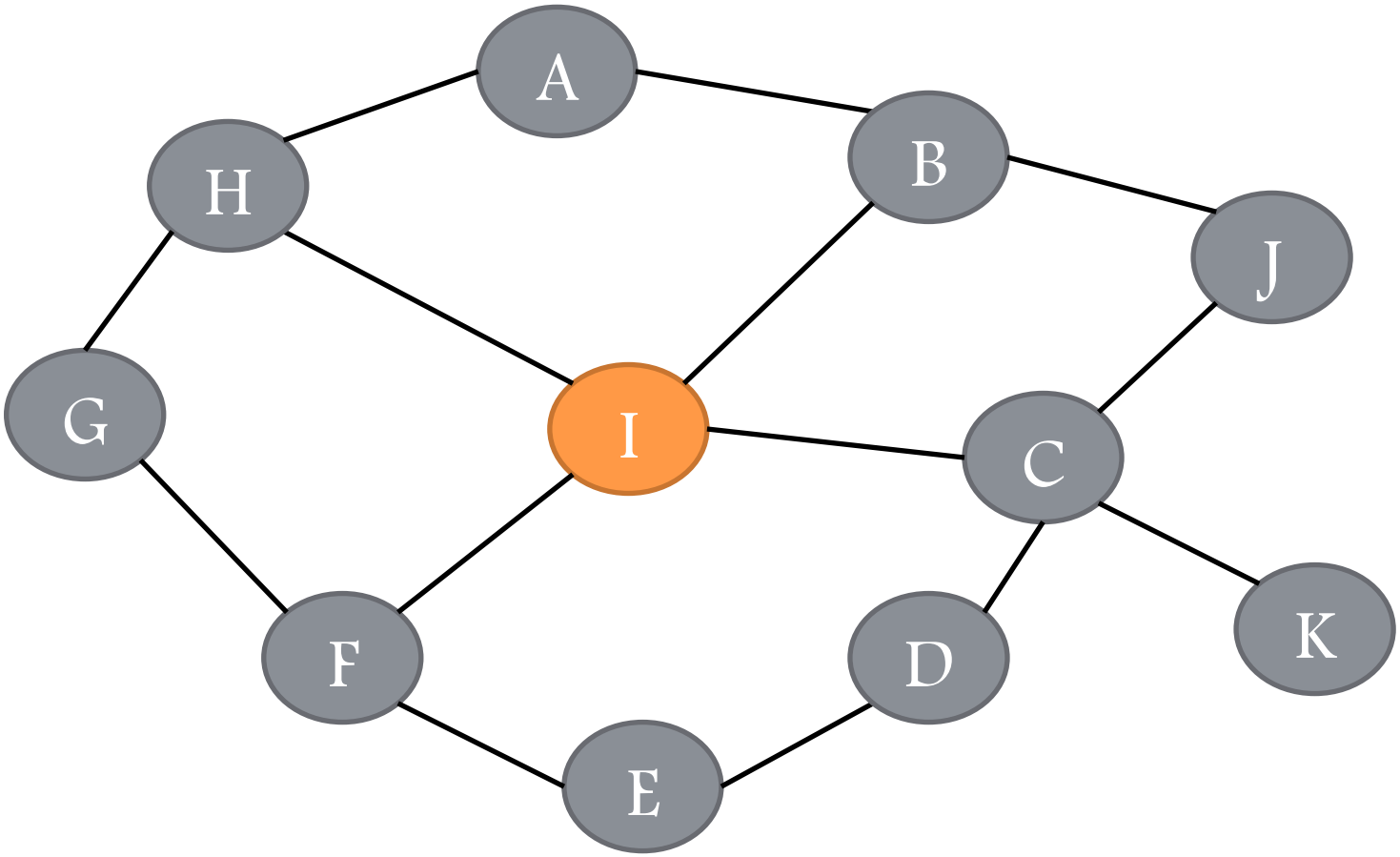
- Paramètre très important qui donne une idée sur la force de l'intrus
- On dit que I maintient la communication entre A et B si I est l'unique utilisateur qui se trouve physiquement entre A et B

- En se trouvant au milieu, I peut mener une attaque active pour détourner le protocole, ce qui renforce ses capacités

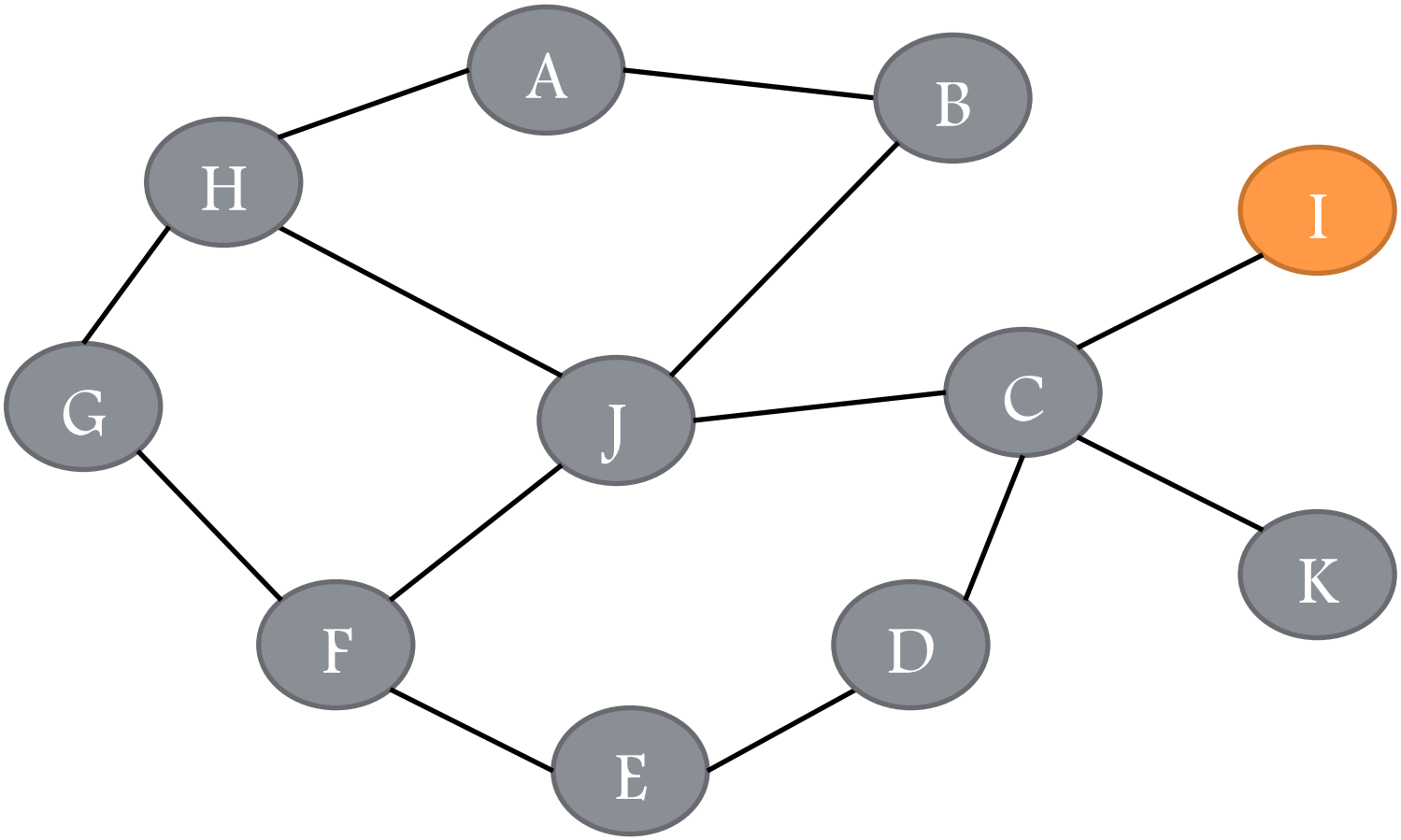
POSITION TRÈS FORTE



POSITION MOINS FORTE



POSITION TRÈS FAIBLE



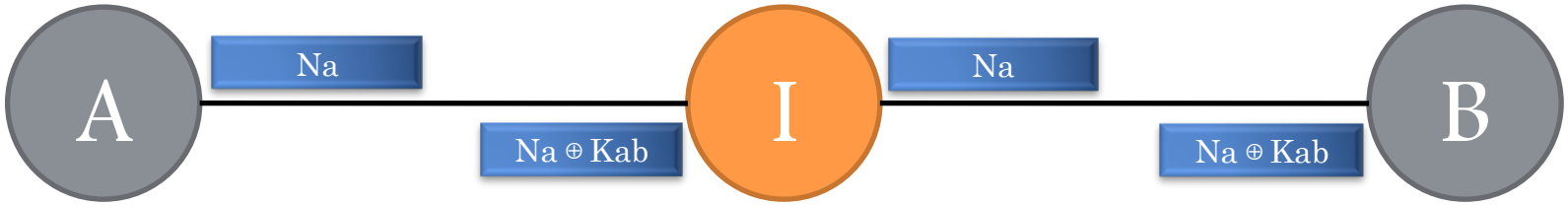
PREUVE DE L'EXISTENCE D'UNE FAILLE

- On dit qu'un protocole d'authentification contient une faille si I arrive à prouver qu'il est autre que I
  - I peut se faire passer pour A s'il arrive à prouver qu'il connaît Kab
- On dit qu'un protocole de confidentialité contient une faille si I est capable de lire les données
- La preuve de l'existence d'une faille est une trace valide de ce protocole montrant que l'objectif visé n'est pas atteint
  - Trace d'exécution valide d'un contre exemple
- Faille à rôle simple
  - Sans changer le rôle d'une session à une autre
- Faille à rôle multiple
  - L'intrus ouvre plusieurs sessions en parallèle

Faille à rôle simple ~ Exemple

1. A → B : Na
2. B → A : $\{Na\}_{Kab}$

L'opérateur de chiffrement : ⊕



Na ⊕ Na ⊕ Kab = Kab

Faille à rôle multiple ~ Exemple

1. $A \rightarrow B : \{Na\}_{Kab}$
2. $B \rightarrow A : \{Na,Nb\}_{Kab}$
3. $A \rightarrow B : \{Nb\}_{Kab}$

1.1 $A \rightarrow I(B) : \{Na\}_{Kab}$

2.1 $I(A) \rightarrow B : \{Na\}_{Kab}$

2.2 $B \rightarrow I(A) : \{Na,Nb\}_{Kab}$

1.2 $I(B) \rightarrow A : \{Na,Nb\}_{Kab}$

1.3 $A \rightarrow I(B) : \{Nb\}_{Kab}$

2.3 $I(A) \rightarrow B : \{Nb\}_{Kab}$

PROTOCOLE DE NEEDHAM ET SCHROEDER

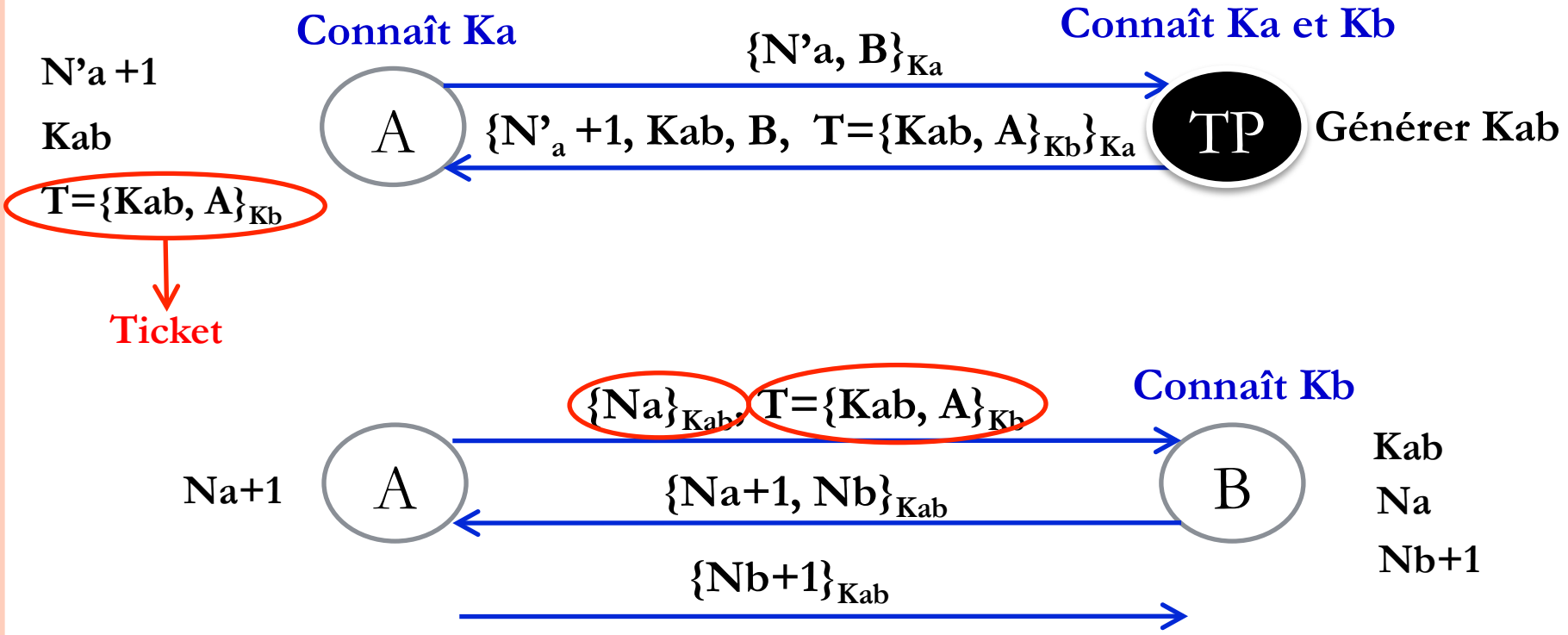
- Inventé par Roger Needham et Michael Schroeder en 1978

Roger Needham

Michael Schroeder

- Distribution de clés symétriques et d'authentification
- Authentification par tierce partie de confiance (TP)
- Notion de tickets

PROTOCOLE DE NEEDHAM ET SCHROEDER



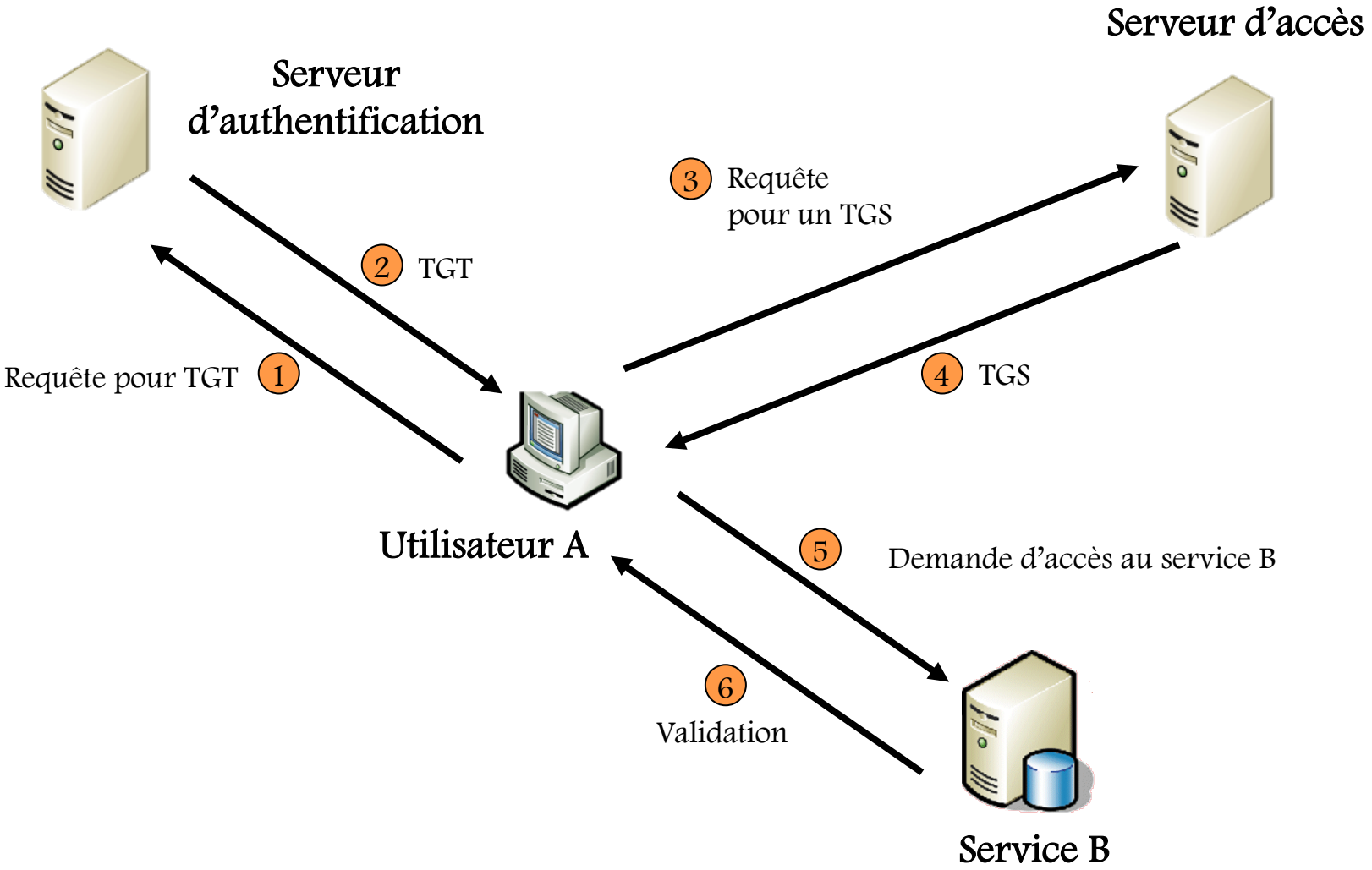
PROTOCOLE DE NEEDHAM ET SCHROEDER

- A demande à TP d'accéder à B et joint $\{N'a, B\}_{Ka}$
- TP génère une clé de session Kab (à partager entre A et B) et répond à A avec $\{N'a+1, Kab, B, T\}_{Ka}$, tel que $T=\{Kab, A\}_{Kb}$
- A déchiffre le message pour avoir T et Kab, et appelle B en lui envoyant T et $\{Na\}_{Kab}$
- B déchiffre T avec Kb pour avoir Kab, ensuite à l'aide de cette dernière déchiffre $\{Na\}_{Kab}$ et répond à A avec $\{Na+1, Nb\}_{Kab}$
- A répond à B avec $\{Nb+1\}_{Kab}$

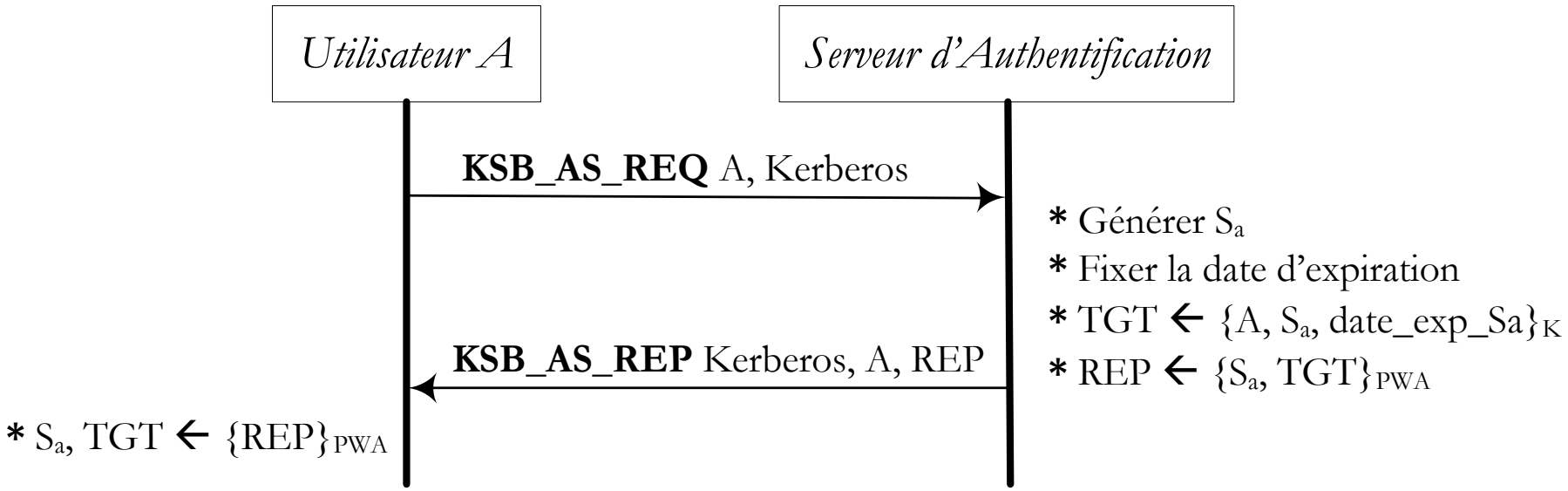
Le système Kerberos

- Deux types de participants :
  - Utilisateur A → possède un mot de passe d'accès PWA
  - Service B → possède un mot de passe d'accès PWB
- Système d'authentification
  - Identification → identifier les utilisateurs et les services
  - Contrôle d'accès → les privilèges d'accès d'un utilisateur à un service
- Il comporte deux sous serveurs :
  - Serveur d'authentification
    - TGT (Ticket Granting Ticket)
    - Ticket pour pouvoir accéder au serveur d'accès
    - Contient une clé de session à partager avec le serveur d'accès
  - Serveur d'accès
    - TGS (Ticket Granting Service)
    - Ticket pour pouvoir accéder à un service donné
    - Contient une clé de session à partager avec le service
  - Les deux serveurs partagent une clé symétrique K

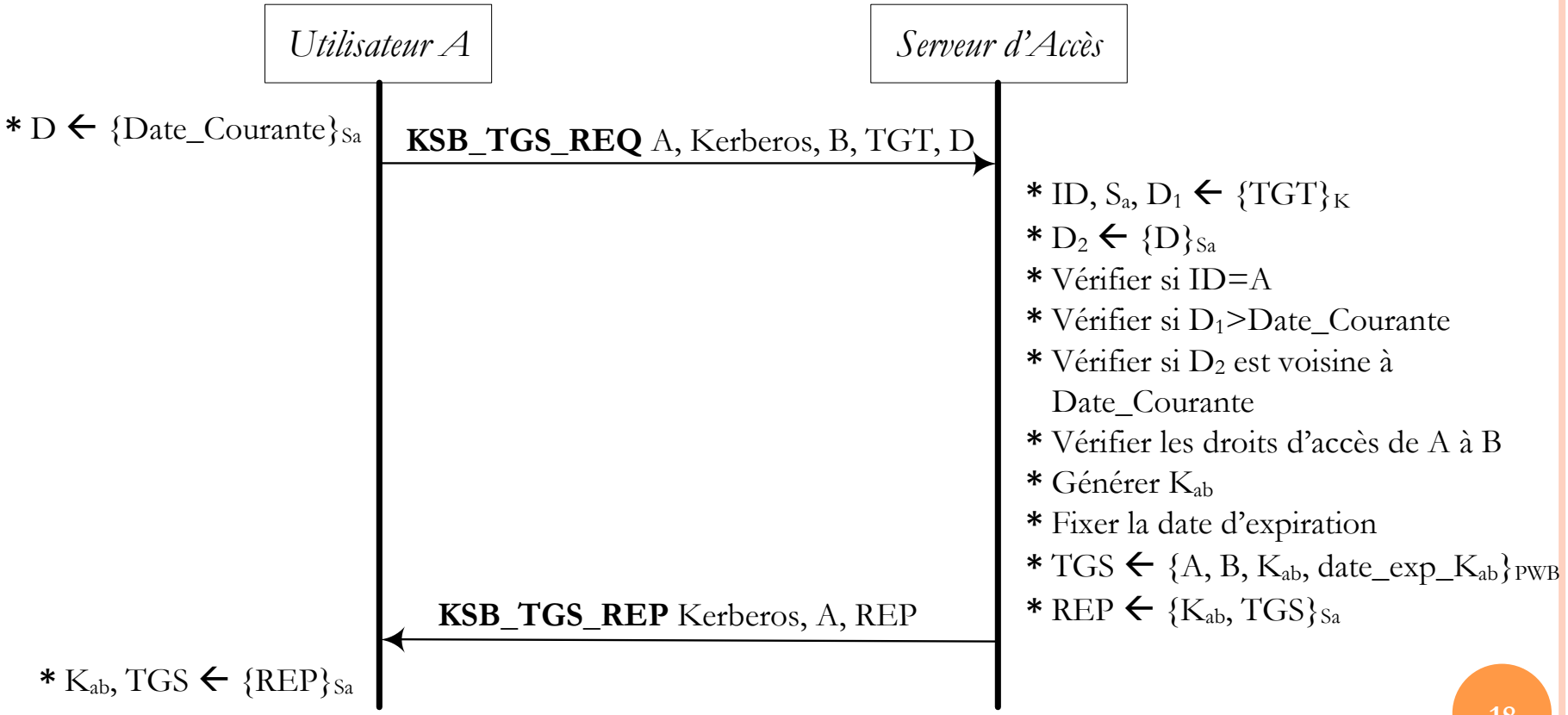
FONCTIONNEMENT DE KERBEROS



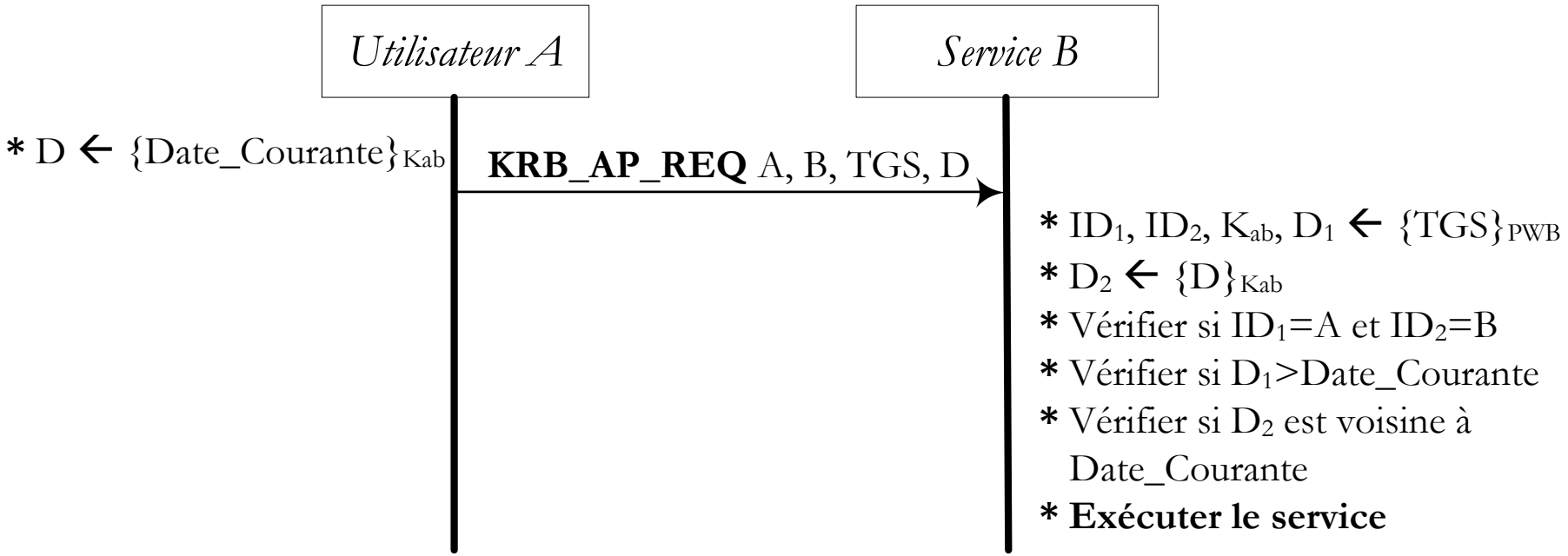
AUTHENTIFICATION DE L'UTILISATEUR



AUTORISATION D'ACCÈS DE L'UTILISATEUR



ACCÈS AU SERVICE



EXERCICE

- Quel est l'avantage d'usage des clés de sessions dans le système Kerberos ?
- Réduire le nombre de clés préétablies
- Pour n utilisateurs et m services :
  - Kerberos → n+m+1 clés
  - Protocoles classiques → n×m clés
- Quel est l'intérêt d'usage des tickets ?
- Pour réduire le nombre de fois l'usage du mot de mot passe pour l'authentification
- Quelle est l'inconvénient de Kerberos par rapport PKI ?
- Le passage à l'échelle
  - Kerberos → un seule serveur pour le réseau entier
  - PKI → délégation