Chapitre IV
Gestion des Clés Symétriques : Cas de Kerberos

Failles des protocoles à clés symétriques

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
- Chaque participant peut activer sur plusieurs sessions d'un même protocole
- Un participant peut changer de rôle d'une session à une autre
- Tous les participants légitimes se comportent conformément à la spécification du protocole

Capacité de l'intrus

- Peut être un participant régulier
- Peut écouter les messages qui circulent sur le réseau
- Peut éliminer ou modifier les messages qu'il intercepte
- Peut générer ses propres messages
- Tous les messages envoyés par l'intrus appartiennent à sa base de connaissances
  - Les connaissances initiales
  - Les messages interceptés

TERMINOLOGIES

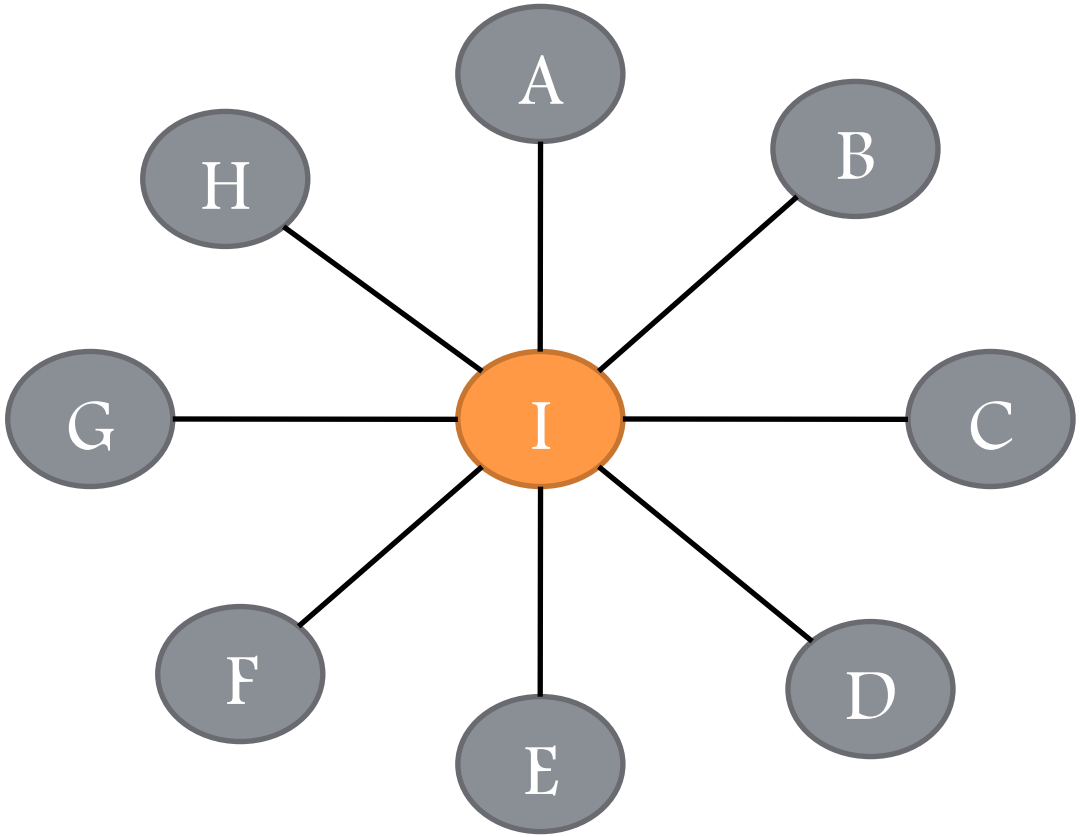
- Nonce ou estampille
  - On note avec Na, un nonce généré par le participant A
  - Une valeur générée d'une façon aléatoire à chaque session
  - Fraicheur de la session de communication
- Clés de chiffrement
  - Clé symétrique : avec laquelle on chiffre et déchiffre les messages
  - On note avec Kab, une clé symétrique partagée entre A et B
  - On note avec Ka, une clé symétrique connue que par A
- Chiffrement
  - On note avec $\{M\}_{Kab}$, un message M chiffré avec la clé Kab
- On note avec I(X), l'intrus qui essaie d'exécuter un protocole en se faisant passer pour le participant X

TOPOLOGIE DU RÉSEAU

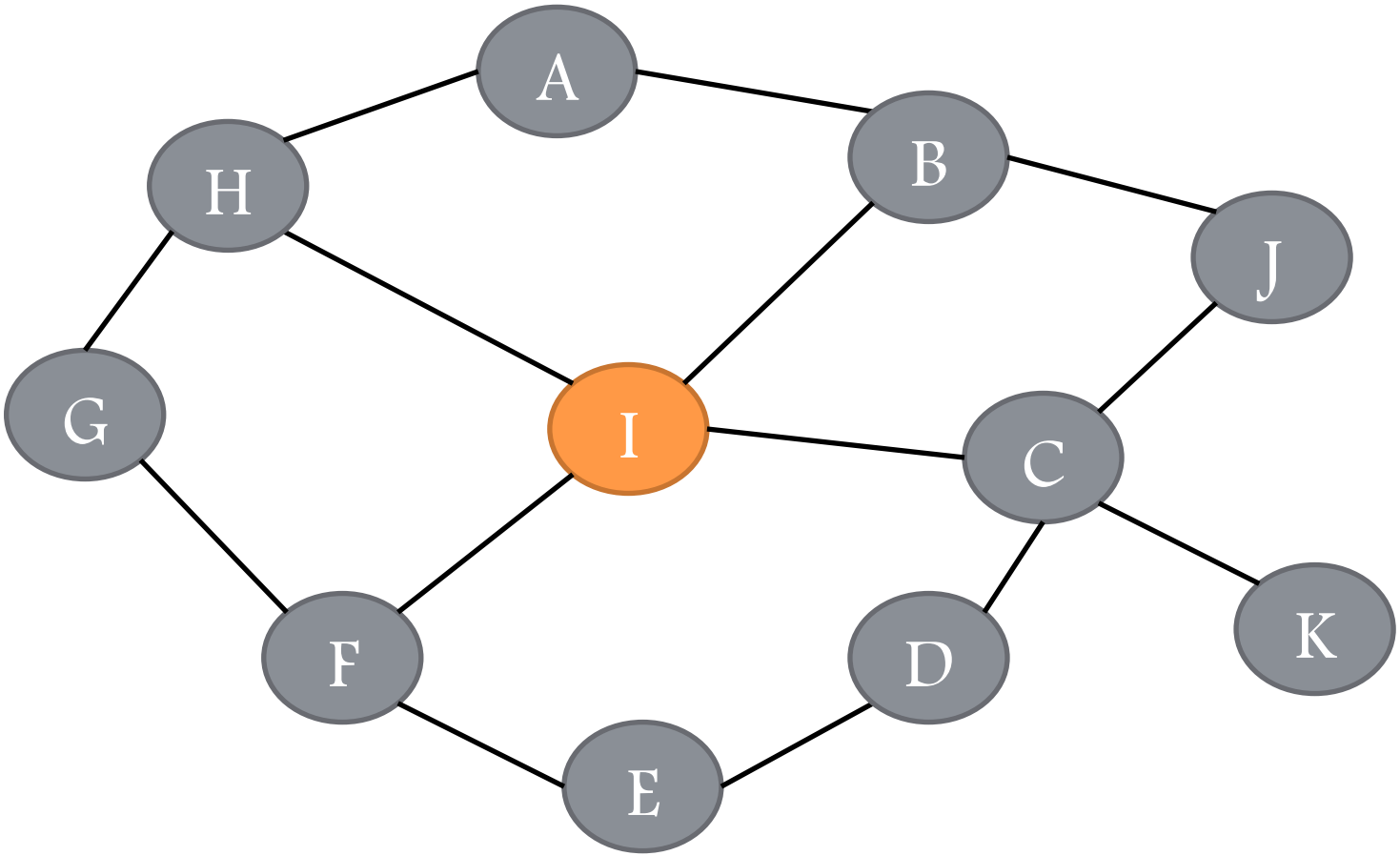
- Paramètre très important qui donne une idée sur la force de l'intrus
- On dit que I maintient la communication entre A et B si I est l'unique entité qui se trouve physiquement entre A et B

- I peut mener une attaque active pour détourner le protocole, ce qui renforce ses capacités

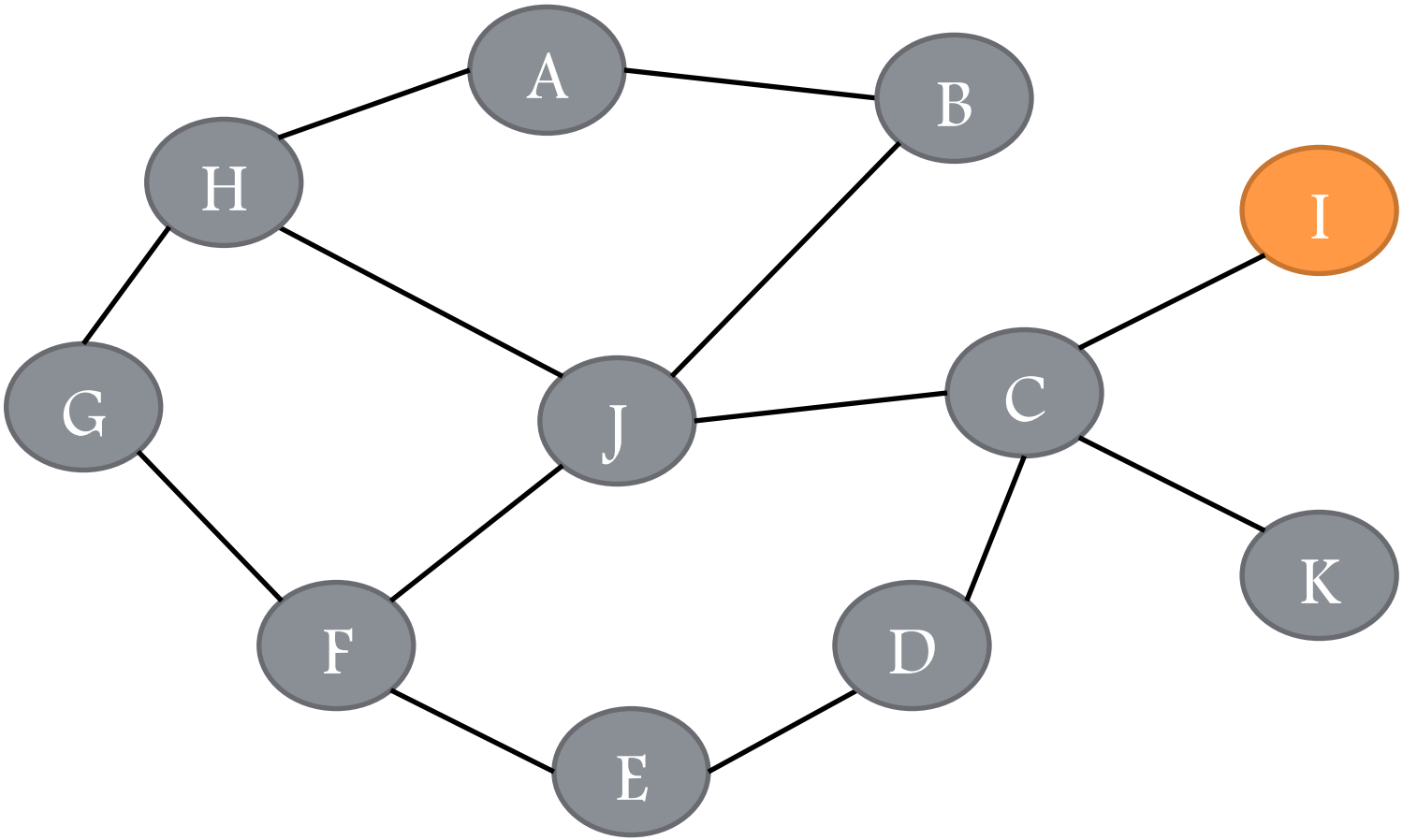
POSITION TRÈS FORTE



POSITION MOINS FORTE



POSITION TRÈS FAIBLE



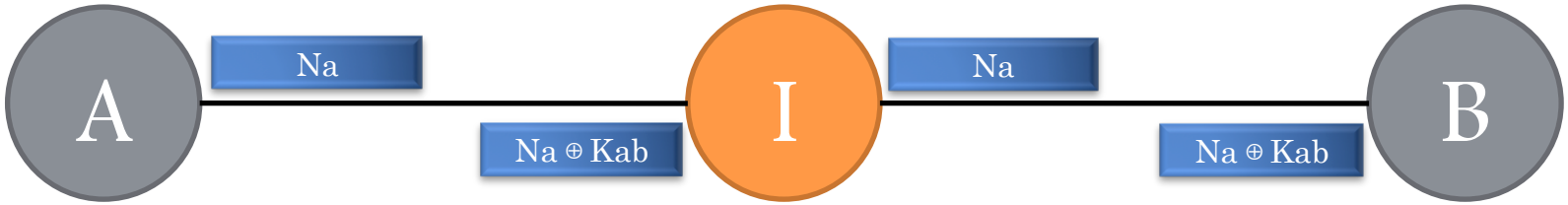
PREUVE D'EXISTENCE D'UNE FAILLE

- On dit qu'un protocole d'authentification contient une faille, si I arrive à prouver qu'il est autre que I
  - I peut s'authentifier en tant que A auprès de B, s'il arrive à prouver à B qu'il connaît la clé Kab
- On dit qu'un protocole de confidentialité contient une faille, si I arrive à lire les données sensées être confidentielles
- La preuve d'existence d'une faille est une trace valide du protocole montrant que l'objectif visé n'est pas atteint (à travers un contre exemple)
- Faille à rôle simple
  - Avec une seule session ouverte du protocole
- Faille à rôle multiple
  - Avec plusieurs sessions ouvertes en parallèle

Exemple 1 (faille à rôle simple)

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

L'opérateur de chiffrement : $\oplus$



$Na \oplus Na \oplus Kab = Kab$

EXEMPLE 2 (FAILLE À RÔLE MULTIPLE)

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

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

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

2.2 $B \rightarrow I(A) : \{Na+1\}_{Kab}$

1.2 $I(B) \rightarrow A : \{Na+1\}_{Kab}$

I s'est authentifié en tant que B auprès de A

PROTOCOLE DE NEEDHAM ET SCHROEDER

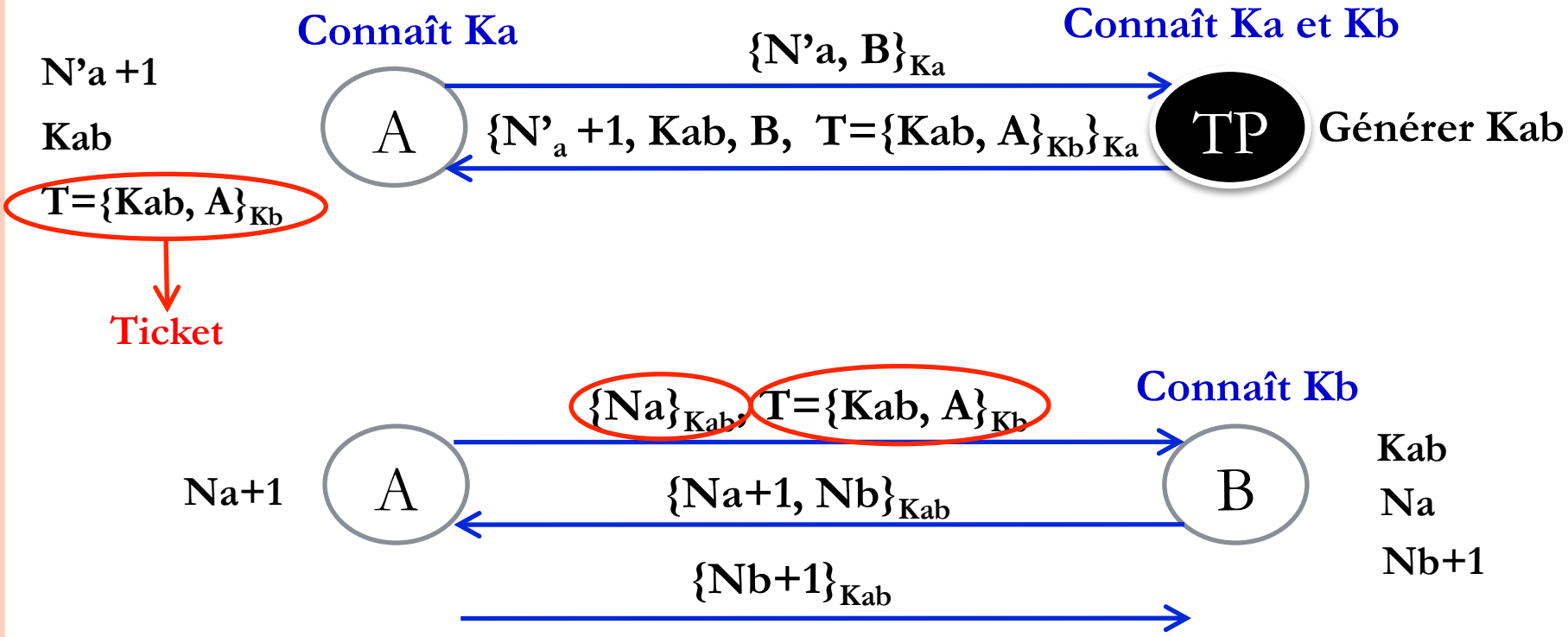
- Inventé par Roger Needham et Michael Schroeder en 1978

Roger Needham

Michael Schroeder

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

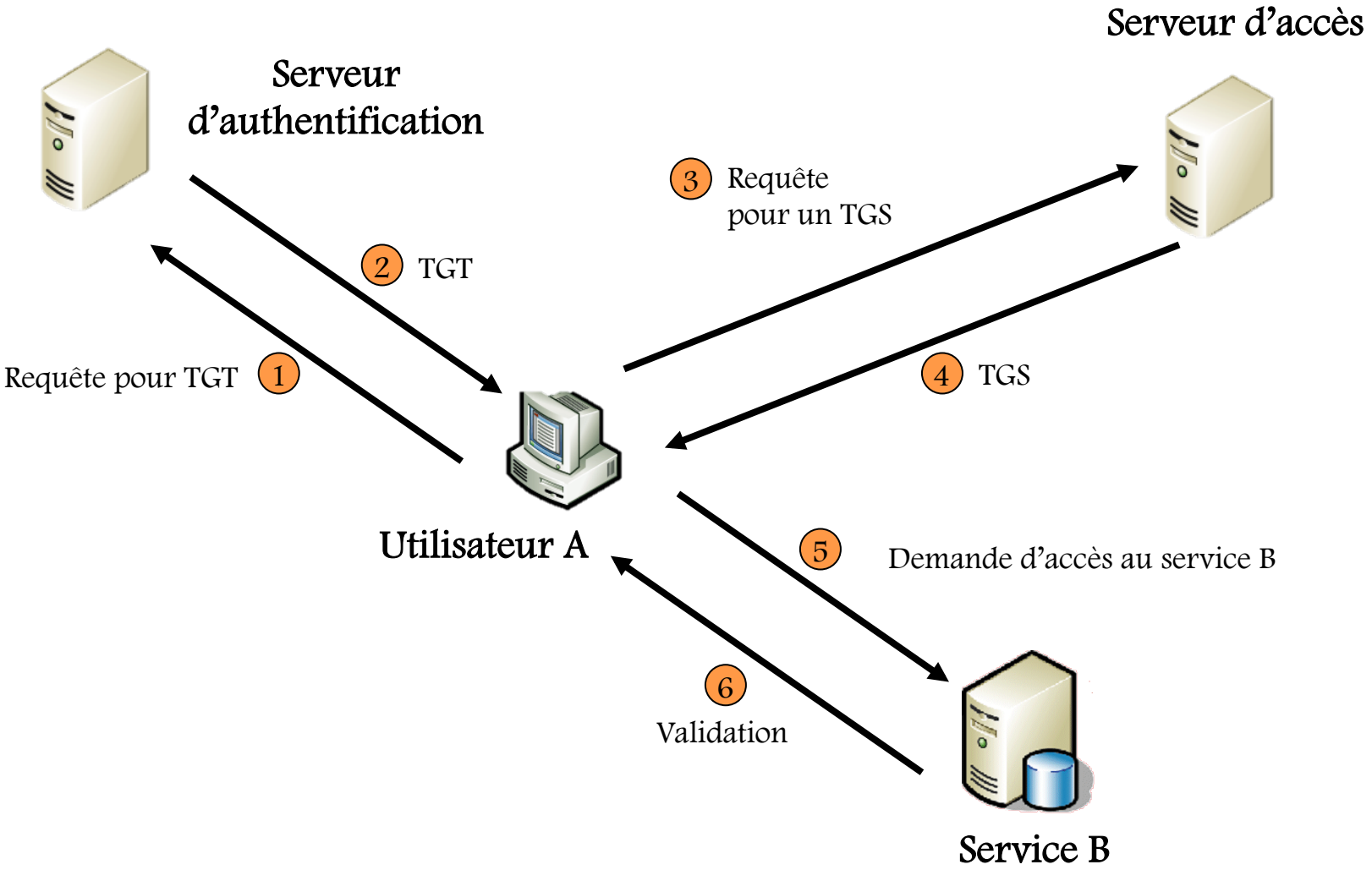
PROTOCOLE DE NEEDHAM ET SCHROEDER



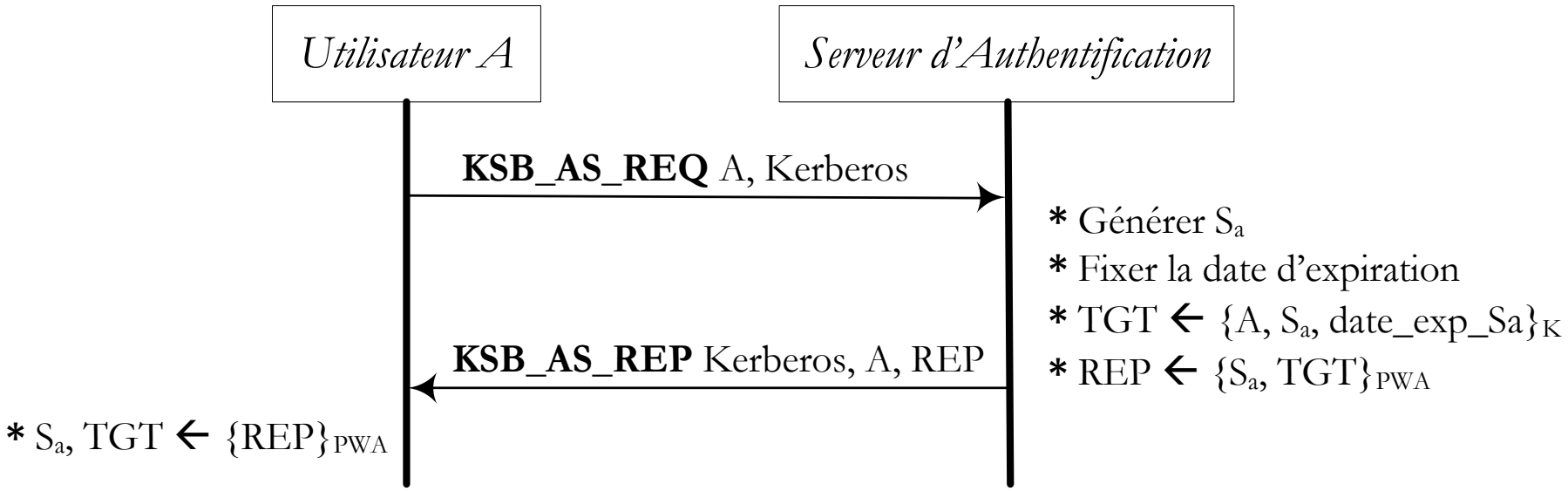
LE SYSTÈME KERBEROS

- Deux types de participants
  - A : Utilisateur (possède un mot de passe d'accès PWA)
  - B : Service (possède un mot de passe d'accès PWB)
- Services de sécurité
  - L'authentification et le contrôle d'accès
- Composé de deux serveurs qui partage une clé K
  - Serveur d'authentification
    - TGT (Ticket Granting Ticket)
    - Contient une clé de session à partager avec le serveur d'accès
  - Serveur d'accès
    - TGS (Ticket Granting Service)
    - Contient une clé de session à partager avec le service

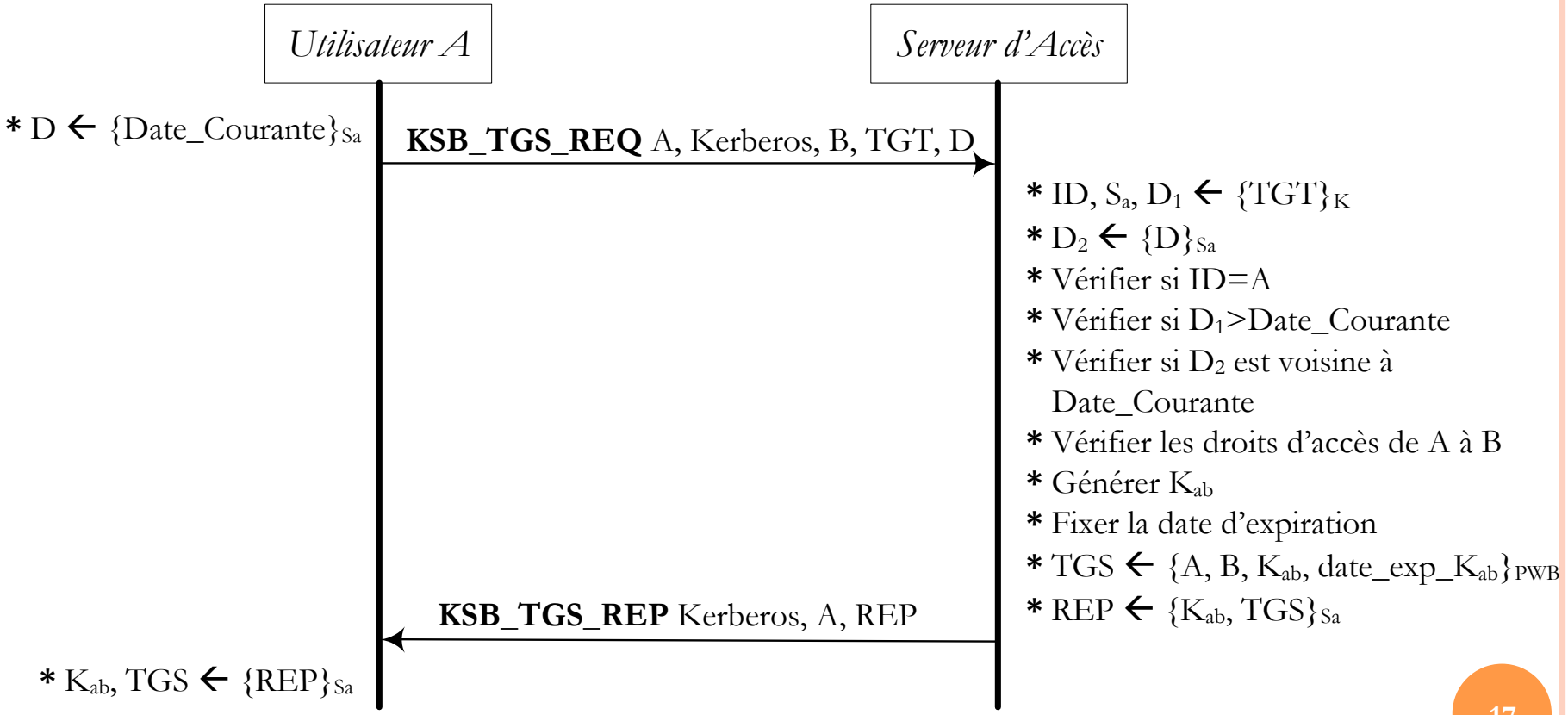
FONCTIONNEMENT DE KERBEROS



AUTHENTIFICATION DE L'UTILISATEUR



AUTORISATION D'ACCÈS DE L'UTILISATEUR



ACCÈS AU SERVICE