Sécurité des Systèmes d'Information(suite)

Nadia BENNANI*- Didier DONSEZ**
Université de Valenciennes
**Institut des Sciences et Techniques de Valenciennes
*IUT de Valenciennes
e-mail : {donsez,nbennani}@univ-valenciennes.fr

Protocoles Cryptographiques

Sommaire

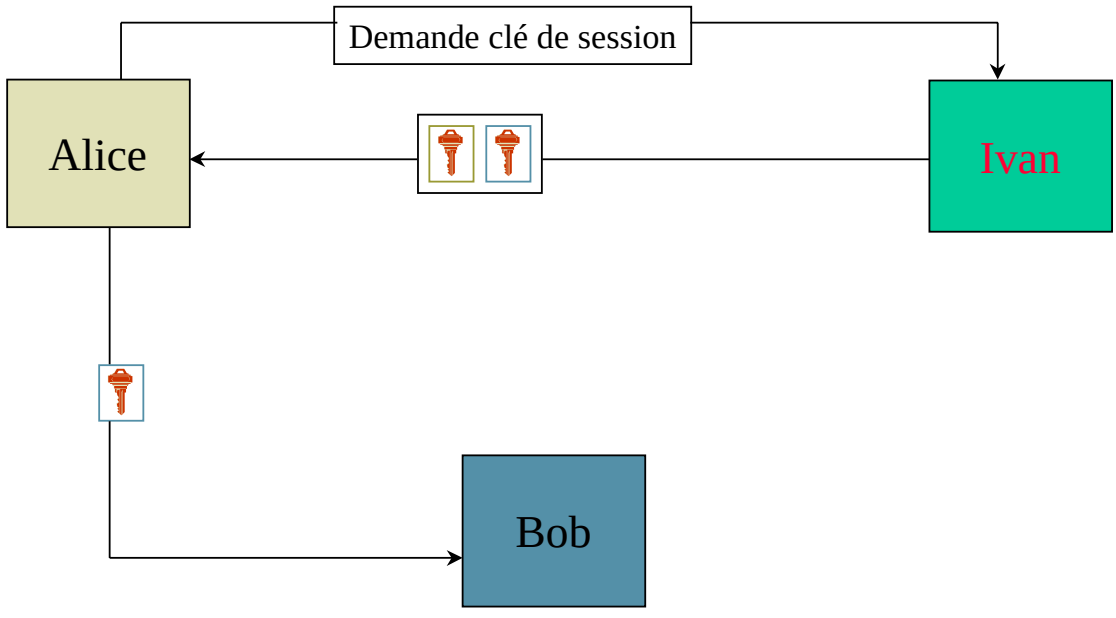
- Protocoles de transmission de clé de session
- Protocoles d'authentification
- Protocoles d'authentification & échange de clés
- Protocoles de datation
- Le protocole de certification X.509
- La signature

Protocoles de transmission des clés de session

- Cryptosystèmes à clé secrète
- Cryptosystèmes à clé publique
- Protocole à cliquets

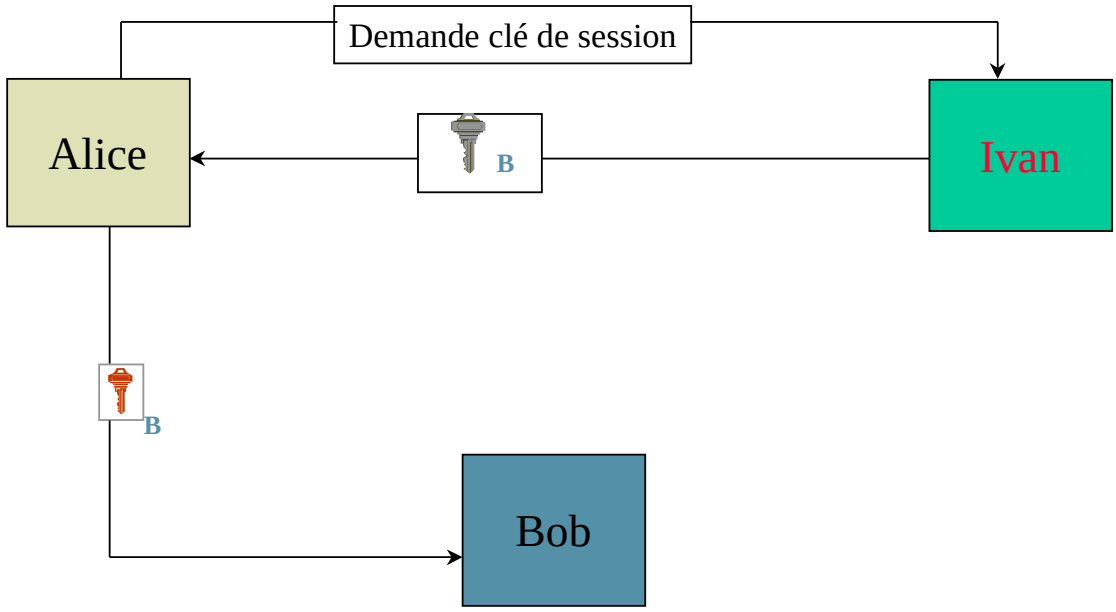
Protocoles de transmission des clés de session

Cryptosystèmes à clé secrète



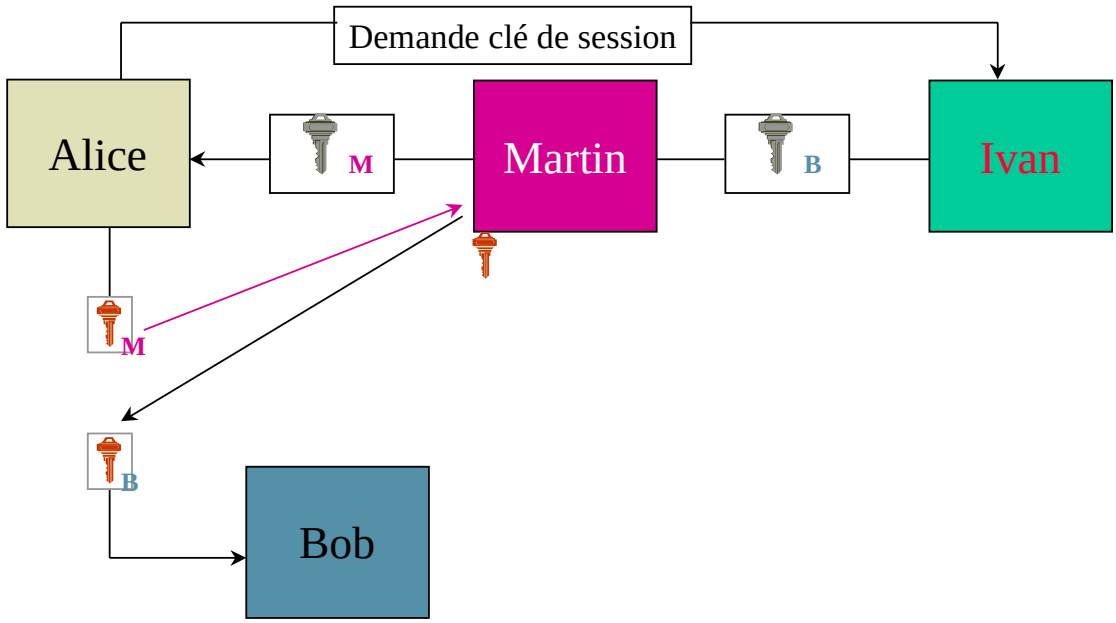
Protocoles de transmission des clés de session

Cryptosystème à clé publique



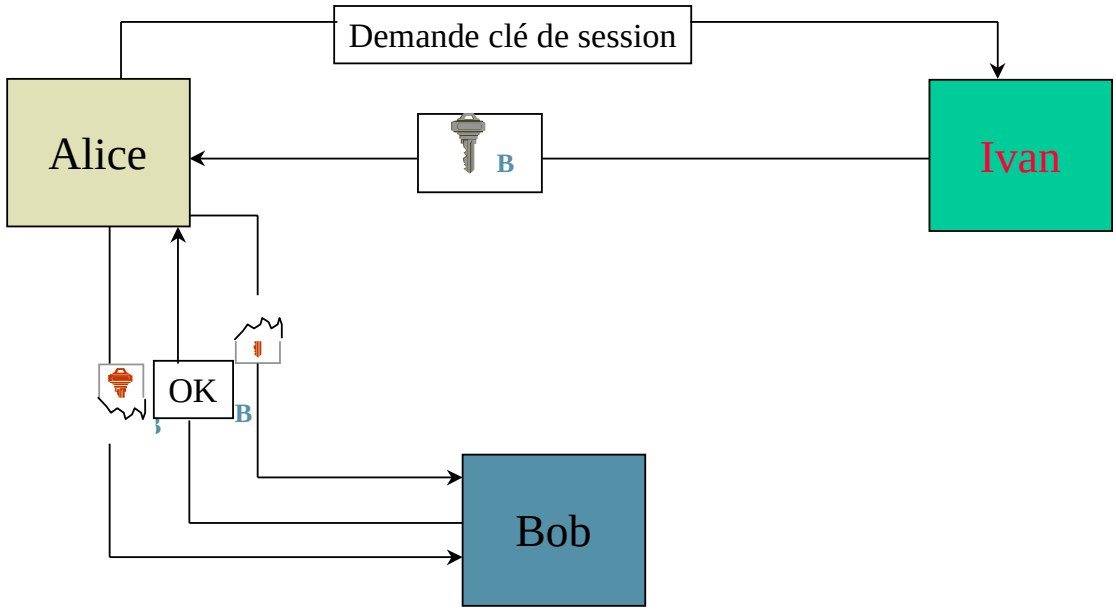
Protocoles de transmission des clés de session

Attaque par l'intercepteur



Protocoles de transmission des clés de session

Protocole à cliquets



Protocoles Cryptographiques

Sommaire

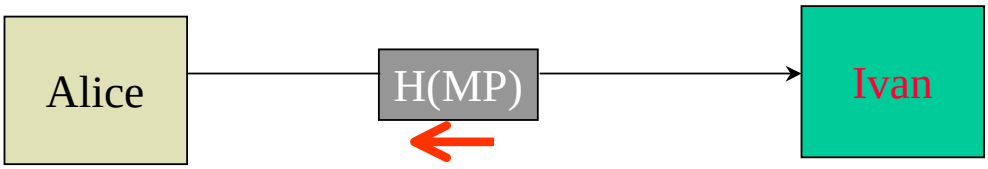
- Protocoles de transmission de clé de session
- **Protocoles d'authentification**
- Protocoles d'authentification & échange de clés
- Protocoles de datation
- Le protocole de certification X.509
- La signature

Protocoles d'authentification

- Utilisation d'une empreinte numérique
- Cryptosystème à clé publique
- Le protocole SKEY
- Le protocole SKID

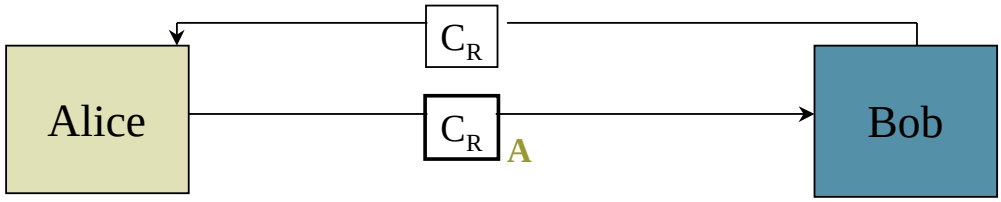
Protocoles d'authentification

Utilisation d'une empreinte numérique



Protocoles d'authentification

Cryptosystème à clé publique



Protocoles d'authentification

Le protocole SKEY

Alice choisit un nombre aléatoire R.
La machine d'Alice calcule: f(R),f(f(R)), ...f^{100}(R).

1ère connexion:
Alice s'identifie à Ivan par : son nom + X100
Ivan calcule f(X100) et compare avec X101 puis stocke X100

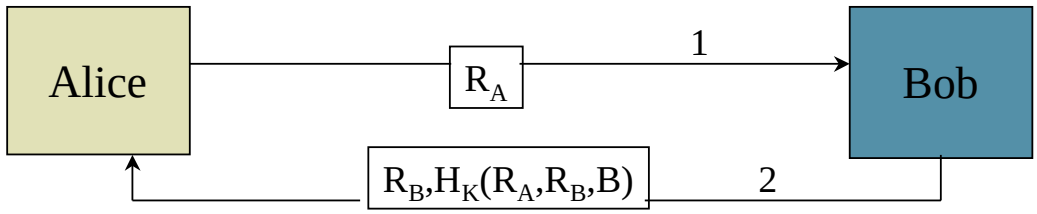
2ème connexion:
Alice s'identifie à Ivan par : son nom + X99
Ivan calcule f(X99) et compare avec X100 puis stocke X99.

....

Protocoles d'authentification

Le protocole SKID

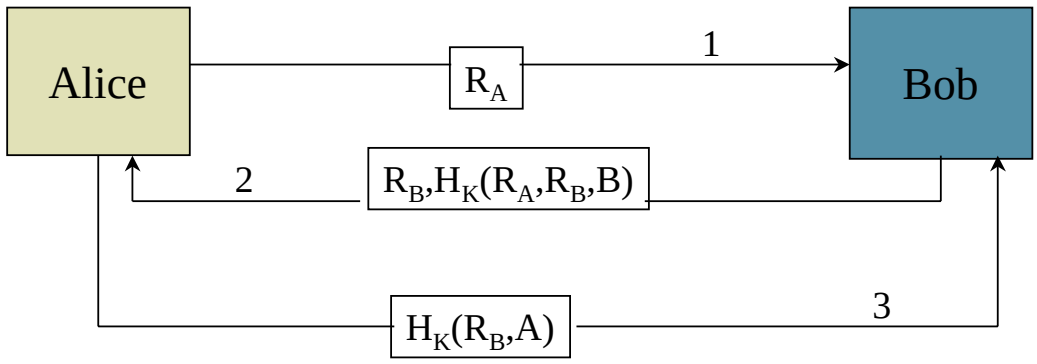
SKID2



Protocoles d'authentification

Le protocole SKID

SKID3



Protocoles Cryptographiques

Sommaire

- Protocoles de transmission de clé de session
- Protocoles d'authentification
- **Protocoles d'authentification & échange de clés**
  - **Cryptosystèmes à clé secrète**
  - Cryptosystèmes à clé publique
- Protocoles de datation
- Le protocole de certification X.509
- La signature

Authentification & échange de clés

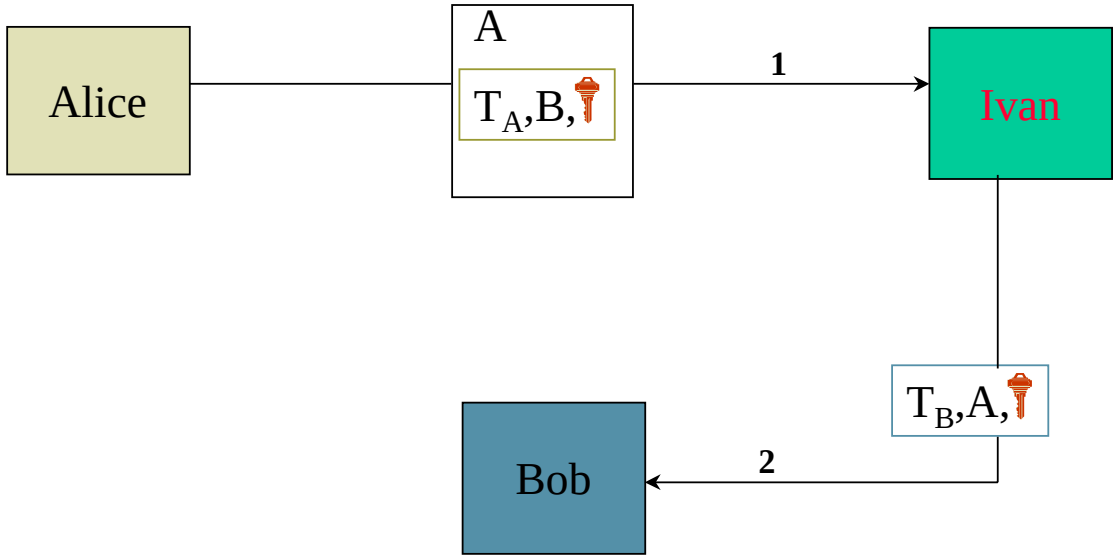
Cryptosystème à clé secrète

- Wide-Mouth-Frog
- Yahalom
- Needam & Schroeder
- Kerberos
- Neuman stubblebine

Authentification & échange de clés

Cryptosystème à clé secrète

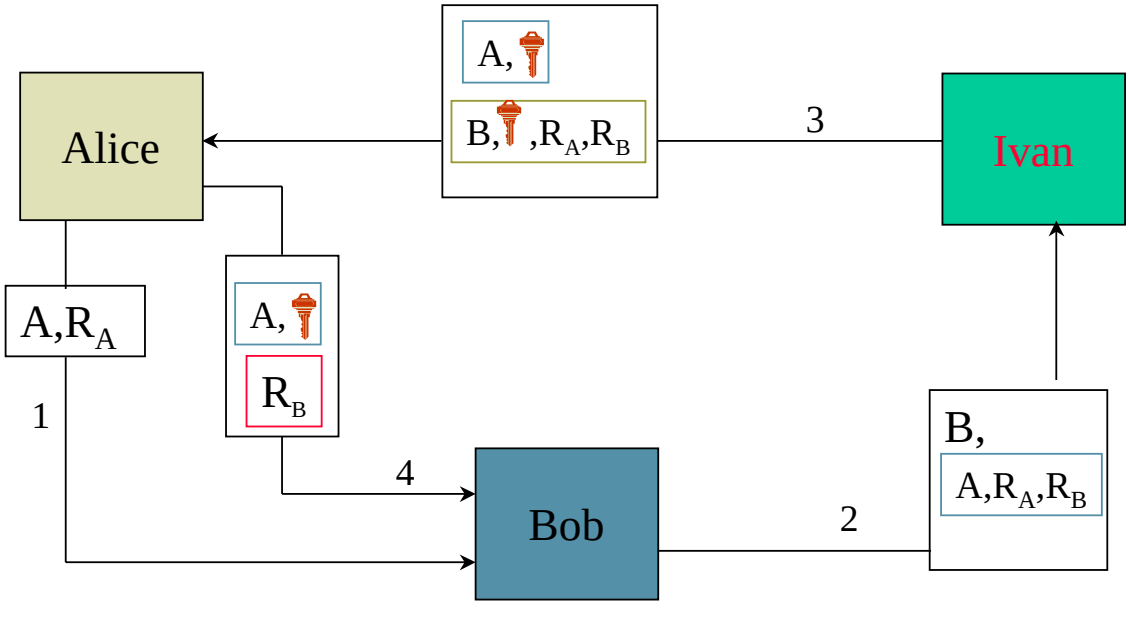
- Wide-Mouth-Frog



Authentification & échange de clés

Cryptosystème à clé secrète

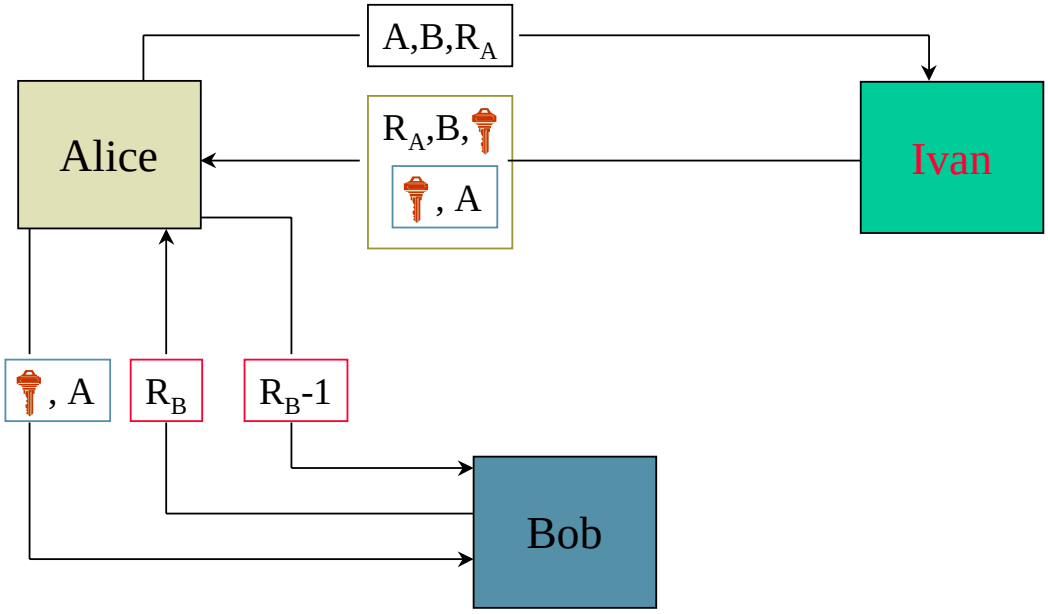
- Yahalom



Authentification & échange de clés

Cryptosystème à clé secrète

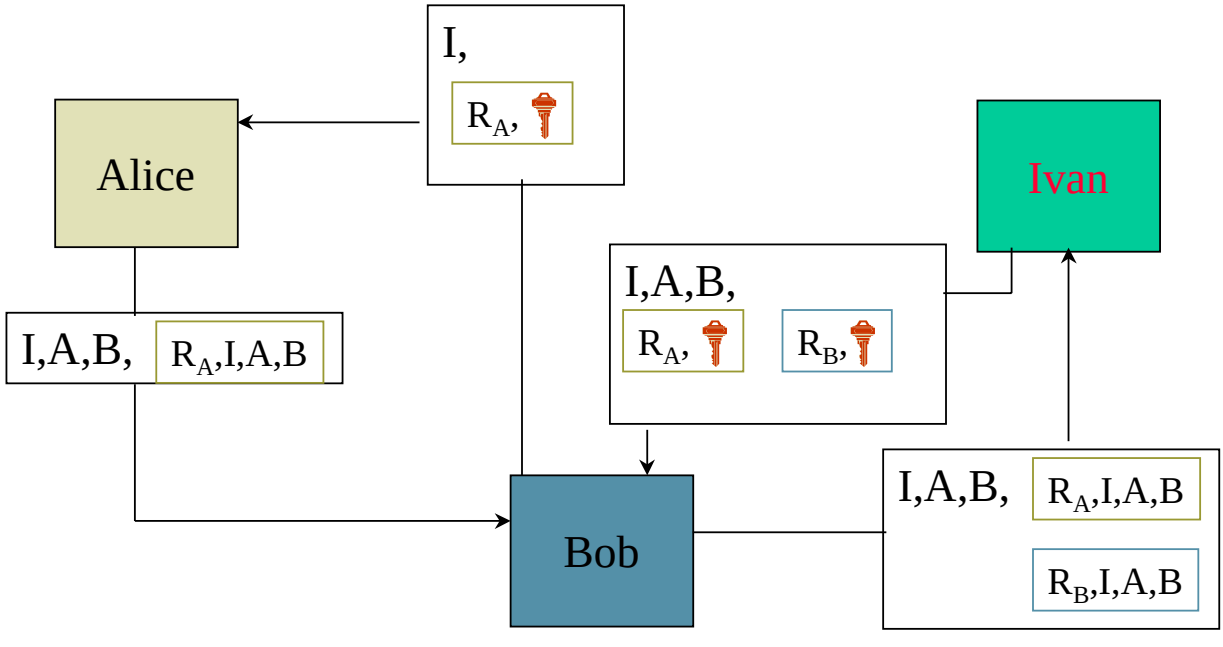
- Needam & Schroeder



Authentification & échange de clés

Cryptosystème à clé secrète

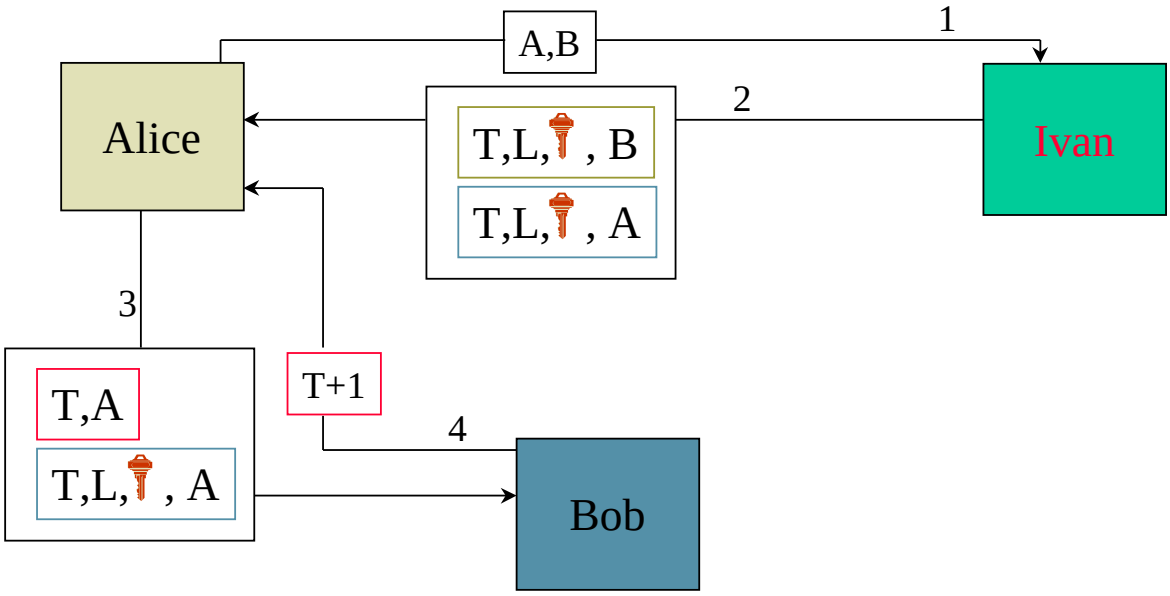
- Otway-Rees



Authentification & échange de clés

Cryptosystème à clé secrète

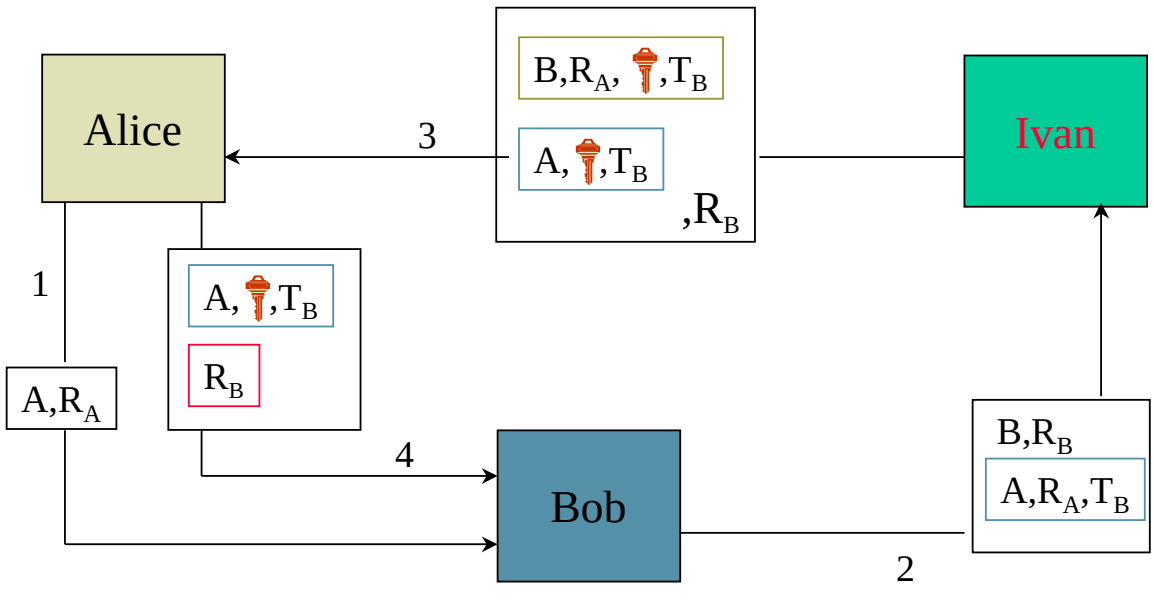
- Kerberos



Authentification & échange de clés

Cryptosystème à clé secrète

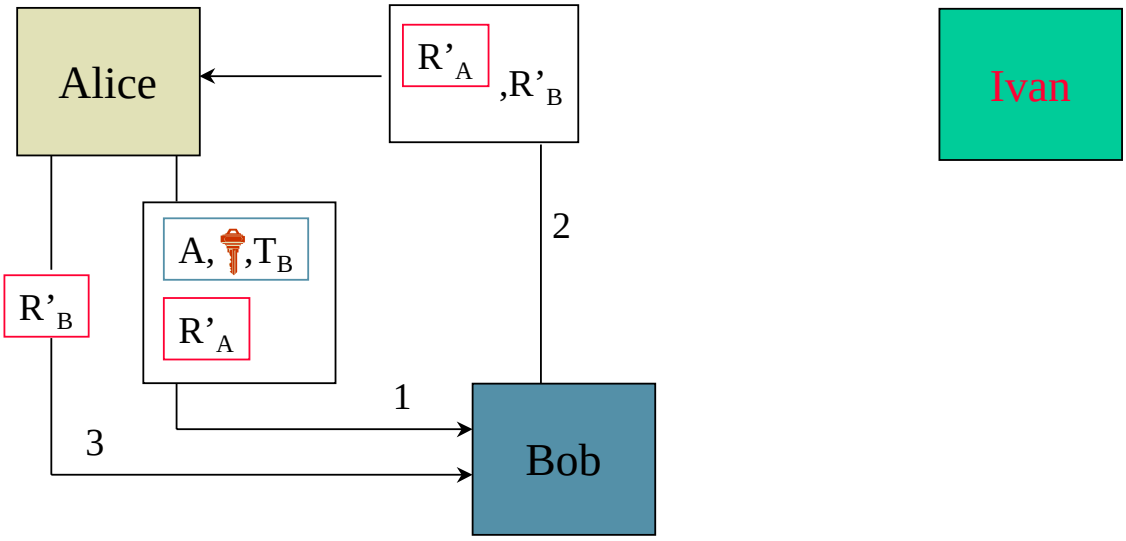
- Neuman stubblebine



Authentification & échange de clés

Cryptosystème à clé secrète

- Neuman stubblebine (protocole bis)



Protocoles Cryptographiques

Sommaire

- Protocoles de transmission de clé de session
- Protocoles d'authentification
- **Protocoles d'authentification & échange de clés**
  - Cryptosystèmes à clé secrète
  - **Cryptosystèmes à clé publique**
- Protocoles de datation
- Le protocole de certification X.509
- La signature

Authentification & échange de clés

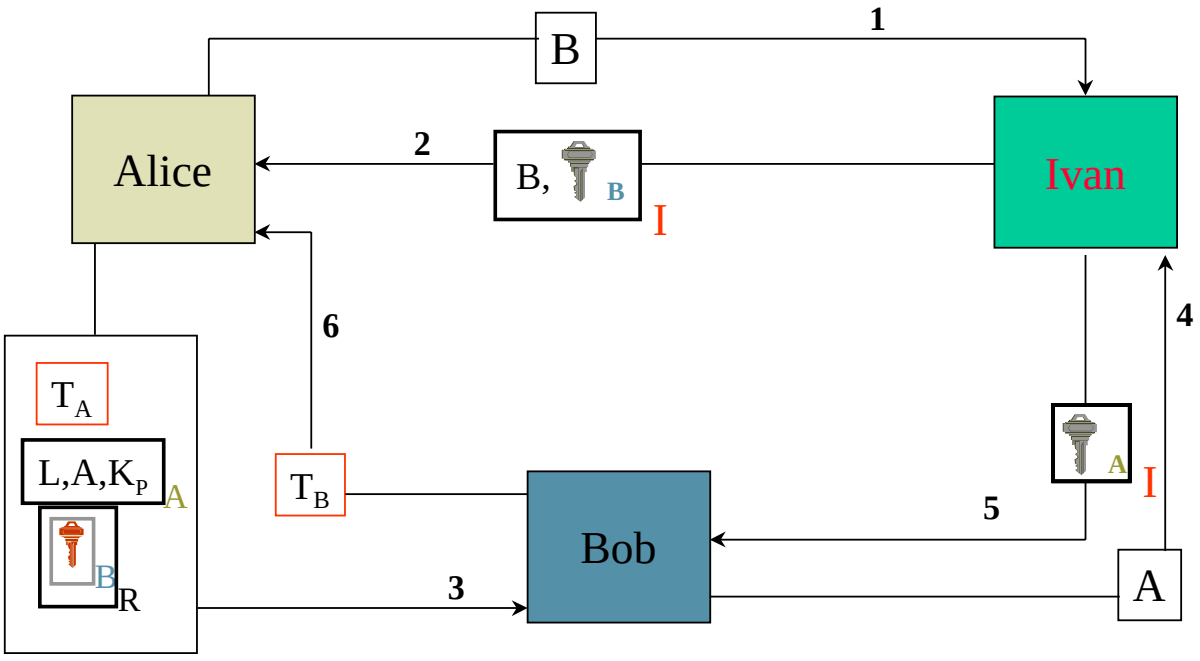
Cryptosystème à clé publique

- DASS
- Denning & Sacco
- Woo - Lam

Authentification & échange de clés

Cryptosystème à clé publique

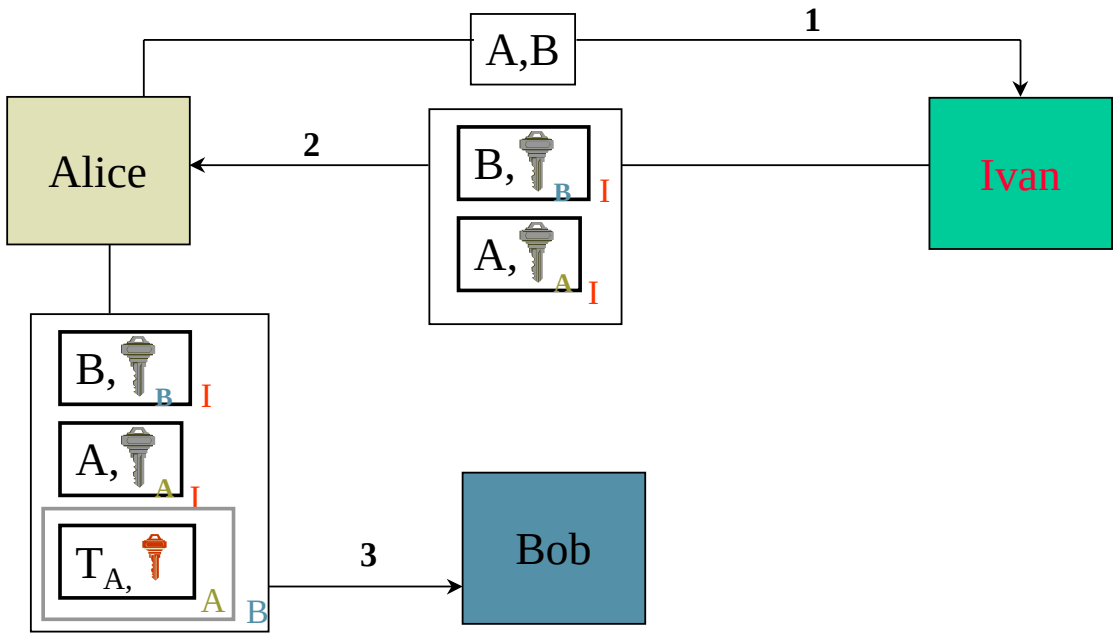
- DASS



Authentification & échange de clés

Cryptosystème à clé publique

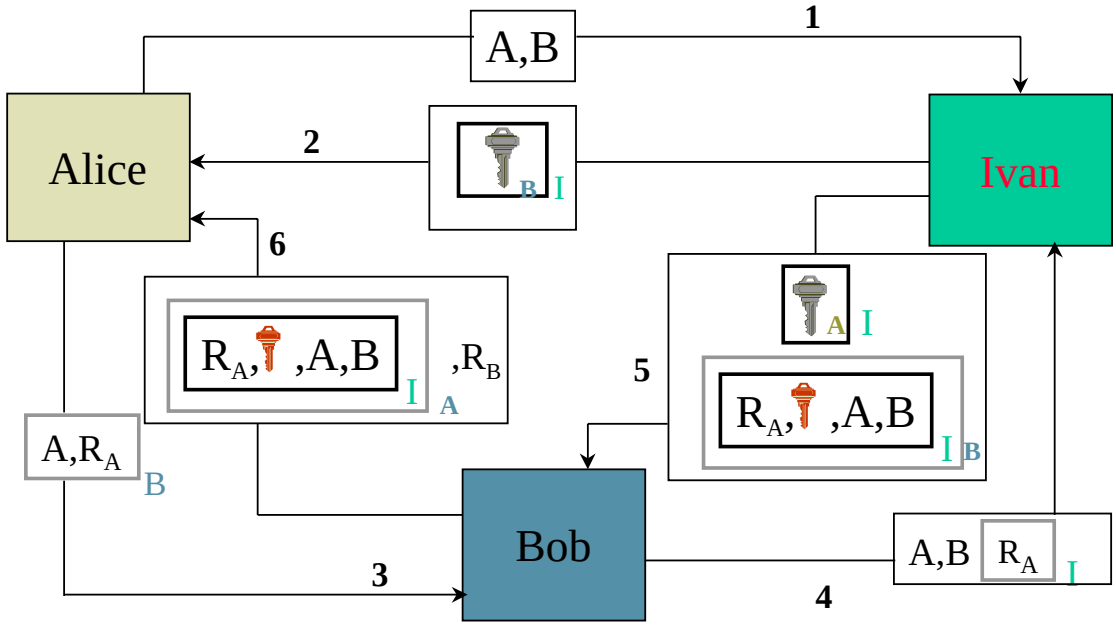
- Denning & Sacco



Authentification & échange de clés

Cryptosystème à clé publique

- Woo - Lam



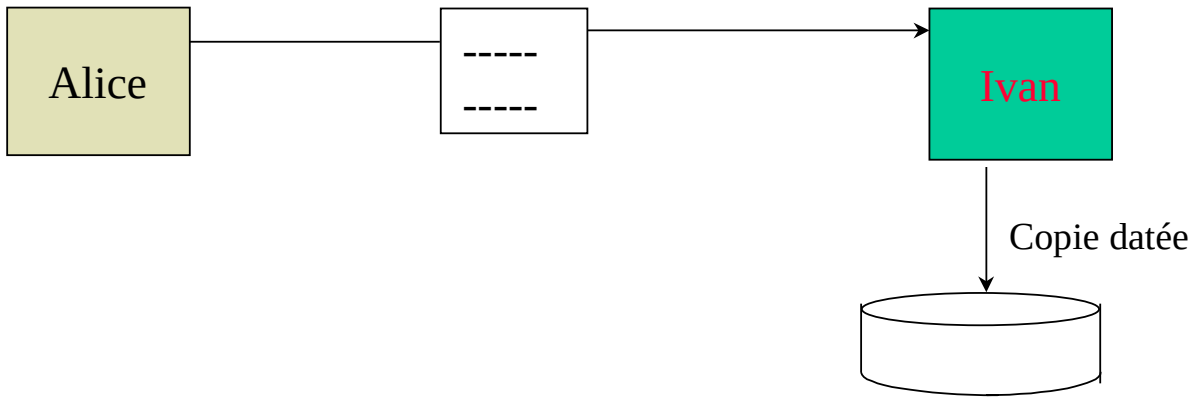
Protocoles Cryptographiques

Sommaire

- Protocoles de transmission de clé de session
- Protocoles d'authentification
- Protocoles d'authentification & échange de clés
  - Cryptosystèmes à clé secrète
  - Cryptosystèmes à clé publique
- **Protocoles de datation**
- Le protocole de certification X.509
- La signature

Protocoles de datation

Datation avec arbitre



Protocoles de datation

Datation avec arbitre

Sauvegarde de tous les documents datés

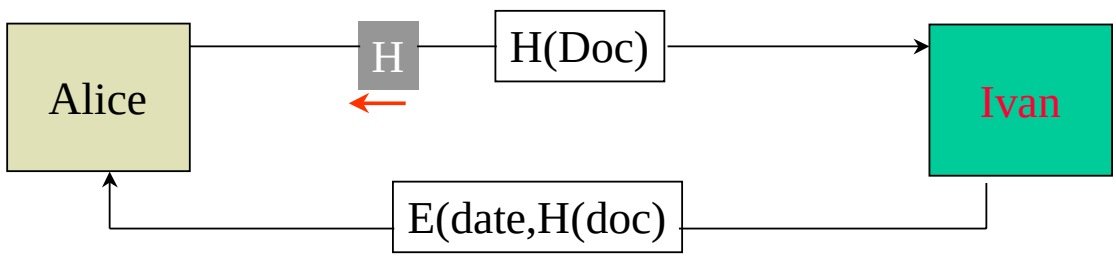
La confidentialité du document n ’est pas préservée

Perte de datation si panne du système d ’Ivan

Risque d ’antidater ou de postdater.

Protocoles de datation

Datation avec arbitre



Protocoles Cryptographiques

Sommaire

- Protocoles de transmission de clé de session
- Protocoles d'authentification
- Protocoles d'authentification & échange de clés
  - Cryptosystèmes à clé secrète
  - Cryptosystèmes à clé publique
- Protocoles de datation
- **Le protocole de certification X.509**
- La signature

Le protocole X.509

Créé en 1988

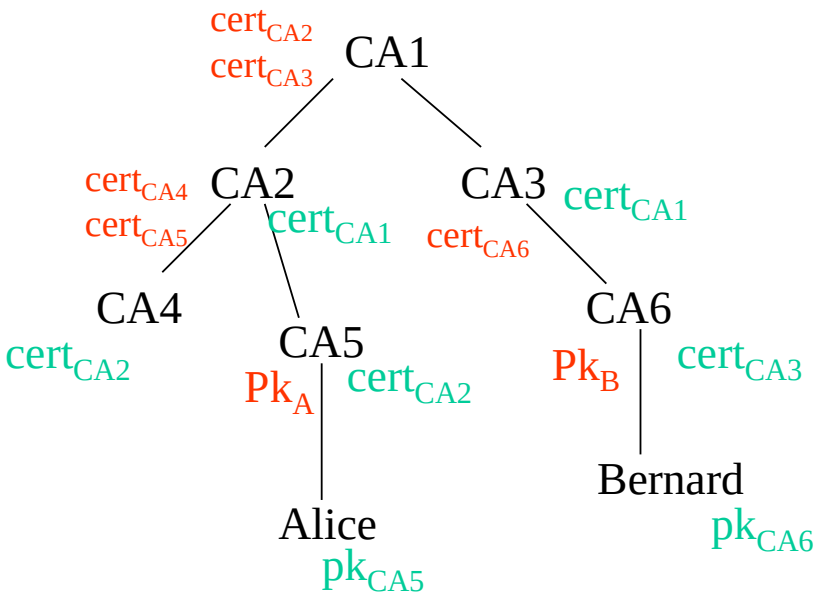
Rôle : Certification des clés publiques.

Format d 'un certificat

Version
N° de série
Algorithme
Autorité certifiante
Période de validité
Utilisateur ou programme
Clé publique

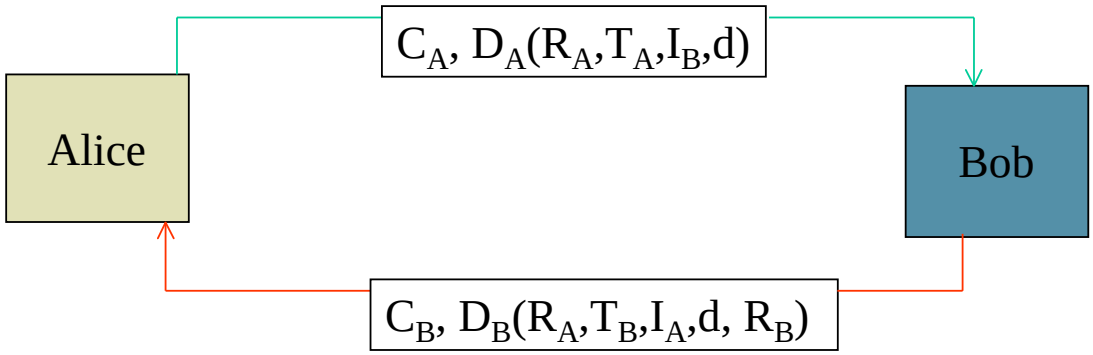
Le protocole X.509

Structure arborescente des CA



Le protocole X.509

Protocole unidirectionnel



La signature en aveugle

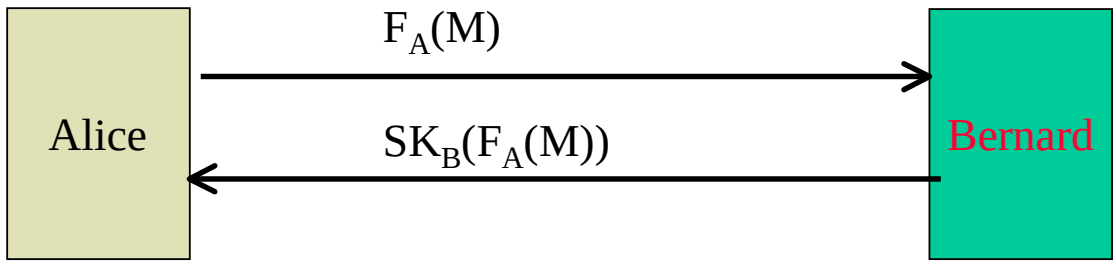
- Principe: Le signature sait « presque ce qu ’il signe.
- Utilisation: La monnaie électronique
- Caractéristique: Anonymat, intraçabilité.

La signature en aveugle total

Alice veut faire signer un document par Bernard

Utilisation d ’un facteur de camouflage : F_A

Protocole



La signature en aveugle

Objectif : Limiter les tentatives de tricherie d ’Alice

Protocole:

1. Alice prépare *n* exemplaires de son document, et les envoie à Bernard.
2. Bernard choisit *n-1* documents et réclame les f. de camouflages correspondants à Alice
3. Bernard vérifie le contenu des n-1 documents.
4. Bernard signe le dernier et l ’envoie à Alice.

La signature en aveugle

5. Alice recalcule le document original signé par Bernard

=> Alice 1 chance sur n de tricher.

Variante

2 ’ - Bernard consulte n/2 messages

4 ’ - Bernard multiplie les n/2 restants et signe le résultat.

La signature en aveugle

Application au commerce électronique

- Le message dans ce cas est une demande de retrait
- Bernard retire le montant demandé par Alice

=> Anonymat de l ’argent électronique

Preuve à divulgation nulle

L’idée: Prouver un fait à quelqu’un mais divulguer l’information à cette personne.