Gestion des Clés

Pr Belkhir Abdelkader

Gestion des clés cryptographiques

1. La génération des clés: attention aux clés faibles, ... et veiller à utiliser des générateurs fiables

2. Le transfert de la clé: se rencontrer, ou utiliser un canal de transmission protégé (difficile sinon impossible), un tiers de confiance

3. La vérification des clés: par hachage, ou utilisation de certificats

4. Le stockage des clés: dans des fichiers, sur supports extérieurs, par surchiffrement

Les échanges de clés de session

Un **protocole d'établissement de clé** est un protocole au cours duquel une clé secrète devient disponible à deux (ou plus) entités

Un **protocole de transport de clé** est un protocole d'établissement de clé où une partie crée ou obtient la clé secrète et la transmet à l'autre (aux autres) partie(s)

Un **protocole d'accord sur la clé** est un protocole d'établissement de clé au cours duquel la clé secrète est dérivée sur base d'information de deux (ou plus, et idéalement : de chaque) parties, de manière à ce qu'aucune partie ne puisse prédéterminer la valeur de la clé secrète ainsi construite

Les échanges de clés symétriques

Un protocole simple d'échange de clé

Si chacune des deux parties A et B a pleine confiance que le message reçu de l'autre partie est en effet authentique, l'échange de la clé de session secrète basé sur un lien de communication sécurisé peut être effectué avec un protocole simple tel que celui décrit ci-dessous:

- Pour communiquer avec B, A génère une paire de clé public/privée notée {PUA, PRA} et transmet un message en clair à B contenant PUA , identificateur de A, IDA (qui peut être l'adresse IP de A).
- A la réception du message de A, B génère et garde une clé secrète KS. Ensuite , il répond à A avec la clé de session secrète KS. Cette réponse à A est chiffrée avec la clé public de A PUA: E(PUA, KS). C'est évident uniquement A peut déchiffrer ce message contenant la clé de session.
- A déchiffre avec sa clé privée PRA le message reçu de B et retrouve la clé de session KS
- A se défait de la paire de clé public/privée {PUA, PRA}, B se défait de PUA

Un protocole simple d'échange de clé (suite)

- Maintenant A et B peuvent communiquer en sécurité en utilisant la clé de session
- Cependant, ce protocole est vulnérable à l'attaque de l'homme du milieu E. Celui-ci est capable d'intercepter les messages entre A et B. L'attaque peut avoir lieu comme suit:
  - Quand A envoie le message en clair contenant PUA et IDA, E intercepte le message (B ne connait pas le message initial)
  - L'adversaire E génère sa propre paire de clé {PUE, PRE} et transmet {PUE, IDA} à B
  - Croyant que le message provient de A, B génère la clé secrète KS, et la chiffre avec PUE et la renvoie à A.
  - Ce message de B est aussi intercepté par E, qui pourra le déchiffrer.
  - Maintenant E chiffre la clé de session KS avec la clé public de A et l'envoie à A.
  - A retrouve la clé secrète et ne suspecte rien, il commence à communiquer avec b en utilisant la clé de session.

Un protocole simple d'échange de clé (suite)

- A retrouve la clé secrète et ne suspecte rien, il commence à communiquer avec b en utilisant la clé de session.
- E peut maintenant prendre connaissance de toute les communications entre a et B

Les échanges de clés symétriques

Diffie-Hellman :

Soient p premier et α un générateur de Z^*_p

$A \rightarrow B : \alpha^x \bmod p$ (avec x valeur aléatoire secrète choisie par Alice)

$B \rightarrow A : \alpha^y \bmod p$ (avec y valeur aléatoire secrète choisie par Bob)

$k = (\alpha^x)^y = (\alpha^y)^x = \alpha^{xy} \bmod p$

Les échanges de clés symétriques

Diffie-Hellman :

Soient p premier et α un générateur de Z^*_p

$A \rightarrow B : \alpha^x \bmod p$ (avec x valeur aléatoire secrète choisie par Alice)

$B \rightarrow A : \alpha^y \bmod p$ (avec y valeur aléatoire secrète choisie par Bob)

$k = (\alpha^x)^y = (\alpha^y)^x = \alpha^{xy} \bmod p$

Les échanges de clés symétriques

Diffie-Hellman : homme au milieu

$$A \rightarrow O : \alpha^x \bmod p$$

$$O \rightarrow B : \alpha^{x'} \bmod p$$

$$B \rightarrow O : \alpha^y \bmod p$$

$$O \rightarrow A : \alpha^{y'} \bmod p$$

Alice calcule $k_1 = (\alpha^{y'})^x \bmod p$

Bob calcule $k_2 = (\alpha^{x'})^y \bmod p$

Oscar calcule :
$k_1 = (\alpha^x)^{y'} \bmod p$ et
$k_2 = (\alpha^y)^{x'} \bmod p$

Les échanges de clés symétriques

Protocole de station à station :

Soient p premier et α un générateur de Z^*_p

$$A \rightarrow B : \alpha^x \bmod p$$

$$B \rightarrow A : \alpha^y \bmod p, E_k(\mathsf{Sig}_B(\alpha^x, \alpha^y))$$

$$A \rightarrow B : E_k(\mathsf{Sig}_A(\alpha^x, \alpha^y))$$

Où $k = (\alpha^x)^y = (\alpha^y)^x = \alpha^{xy} \bmod p$

Les échanges de clés symétriques

Le protocole de Needham-Schroeder:

Cadre : A et B veulent communiquer. A (resp. B) partage avec S la clé secrète K_{AS} (resp. K_{BS})

1. A demande à S une clé de session K_{AB} pour communiquer avec B. Il utilise pour cela un jeton J_A. En résumé
   $A \rightarrow S : A; B; J_A$
2. S renvoie à A la clé de session chiffrée et un certificat pour B.
   $S \rightarrow A : K_{AS}(J_A; B; K_{AB}; K_{BS}(K_{AB}; A))$
3. A envoie le certificat à B
4. B chiffre avec K_{AB} un jeton J_B et l'envoie à A.
5. A chiffre avec K_{AB} une modification simple de J_B, par ex J_B -1 et l'envoie à B.
6. A et B peuvent communiquer avec la clé de session K_{AB}.

Les échanges de clés asymétriques

Problème: l'authentification des utilisateurs liés à ces clés.

- Annonce publique
- Annuaire publiquement disponible
- Autorité de clés publique
- Certificats de clé publique

Annonce Publique

La distribution des clés publiques se fait directement aux destinataires ou par broadcast à la communauté.

le risque majeur: la contrefaçon

n'importe qui peut créer une clef en prétendant être quelqu'un d'autre et la publier. La mascarade continuera tant que la contrefaçon n'est pas découverte.

Annuaire Publique

On enregistre les clés dans un annuaire public, $\Rightarrow$ de faire confiance à cet annuaire.

Annuaire:

– Il doit contenir les entrées {nom, clef publique},

– Il doit être possible de s'inscrire de manière sécurisée dans l'annuaire,

– On doit pouvoir remplacer la clef à tout moment,

– L'annuaire doit être publié périodiquement,

– Il devrait également permettre la consultation électronique.

Les autorités

Les clés secrètes peuvent être gérées et distribuées par une autorité qui sera :

- un **centre de distribution de clés**, si les clés sont générées par l'autorité,
- un **centre de translation de clés**, si chaque clé est générée par un utilisateur et transmise à l'autorité

La vie d'une clé (secrète ou publique)

La **crypto-période** d'une clé est la période au cours de laquelle une clé est valide

Cette crypto-période permet de limiter la durée de validité d'une information chiffrée ou encore de limiter l'usage d'une clé, sachant que sa durée de vie dépend des avancées technologiques

Une clé peut être **à court terme** ou **à long terme**

Infrastructure à clé publique (PKI)

Une autorité de certification (CA) associe à chaque utilisateur un certificat sécurisant ce lien.

Etape 1 : Enregistrement

- Alice donne à l'autorité de certification ses informations personnelles et les prouve (carte d'identité, biométrie, registre, ...)
- CA vérifie les informations
- CA crée un nom d'utilisateur pour Alice

Infrastructure à clé publique (PKI)

Étape 2 : Génération de clé

- CA (ou Alice) engendre une paire clé publique/clé privée
- La clé privée est stockée sur le PSE (Environnement personnel de sécurité) d'Alice et par l'autorité de séquestre (key escrow).
- La clé publique est stockée par CA.

Infrastructure à clé publique (PKI)

Étape 3 : Certification

CA crée un certificat pour Alice qu'il stocke.

Il y a des normes pour les certificats (X.509 par exemple)

Le certificat est une chaîne de caractères, signé par le CA et contenant:

- L'identité d'Alice.
- La (ou les) clé publique d'Alice.
- L'algorithme de clé publique utilisé.
- Un numéro de série.
- Une période de validité.
- Des informations sur le CA.

Affichage Favoris Outils ?

لعبة جيوتى الاستايل) لعبة جيوتى الاستايل La Cloche du vieux Manoir, ... Connexion (2) Kids-Idea Gift List of 3D bows Epic Gingerbread House Co... Jeux de Dora l'Exploratr

Connexion

Page Sécurité Outils

ous suffit de **configurer**

Se connecter

Identifiant Windows Live ID :

exemple555@hotmail.com

Mot de passe :

Votre compte n'est pas accessible ?

Maintenir la connexion

Se connecter

Vous n'êtes pas sur votre ordinateur ?

Obtenir un code à usage unique pour se connecter avec

Hotmail, Messenger,

ails | Chemin d'accès de certification

nformations sur le certificat

ficat est conçu pour les rôles suivants :

t l'identité d'un ordinateur distant

ltez la déclaration de l'Autorité de certification pour plus de détails.

livré à : login.live.com

livré par : VeriSign Class 3 Extended Validation SSL CA

ide à partir du 28/09/2011 **jusqu'au** 28/09/2012

Installer le certificat... | Déclaration de l'émetteur

OK

Connexion - Windows Internet Explorer

https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1334081942&rver=6.1.6206.0&wp=MBI8 Microsoft Corporation [US]

Search the web

Fichier Edition Affichage Favoris Outils ?

2) لعبة جيوتى الاستايل) لعبة جيوتى الاستايل La Cloche du vieux Manoir, ... Connexion (2) Kids-Idea Gift List of 3D bows Epic Gingerbread House Co... Jeu

Favoris Connexion

Page Sécurité

Certificat

Général | Détails | Chemin d'accès de certification

Afficher : <Tout>

Champ	Valeur
Version	V3
Numéro de série	02 9a ee 64 54 95 b8 1d e1 5a...
Algorithme de signature	sha1RSA
Émetteur	VeriSign Class 3 Extended Vali...
Valide à partir du	mercredi 28 septembre 2011 0...
Valide jusqu'au	vendredi 28 septembre 2012 0...
Objet	login.live.com, Passport, Micro...
Clé publique	RSA (2048 Bits)

Modifier les propriétés... Copier dans un fichier...

OK

...us suffit de **configurer**

...tion

...Hotmail, Messenger,

Se connecter

Identifiant Windows Live ID :

exemple555@hotmail.com

Mot de passe :

Votre compte n'est pas accessible ?

Maintenir la connexion

Se connecter

Vous n'êtes pas sur votre ordinateur ?

Obtenir un code à usage unique pour se connecter avec

Centre d'aide | Com

Les certificats de clés publiques

Un **certificat d'une clé publique** consiste en des données et une signature digitale

Les données contiennent (au-moins) la clé publique et un string identifiant de manière unique, l'entité associée à cette clé publique

La signature digitale est réalisée par une autorité de certification sur les données du certificat

La clé publique de vérification de la signature de l'autorité de certification doit être publiquement connue

La révocation

Une clé est **compromise** lorsqu'un adversaire possède de l'information sur des données secrètes

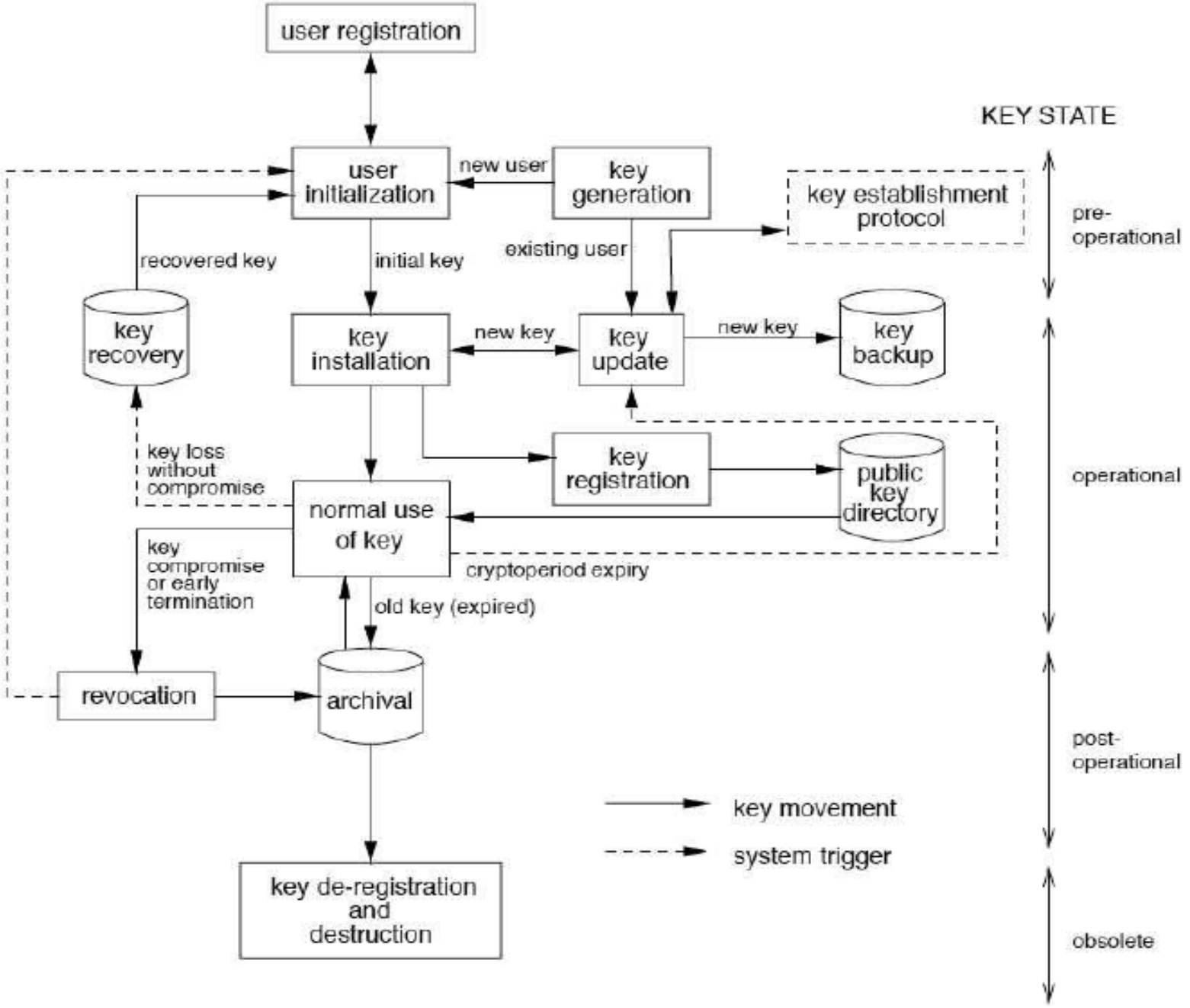
Lorsqu'une clé est compromise, elle doit être révoquée

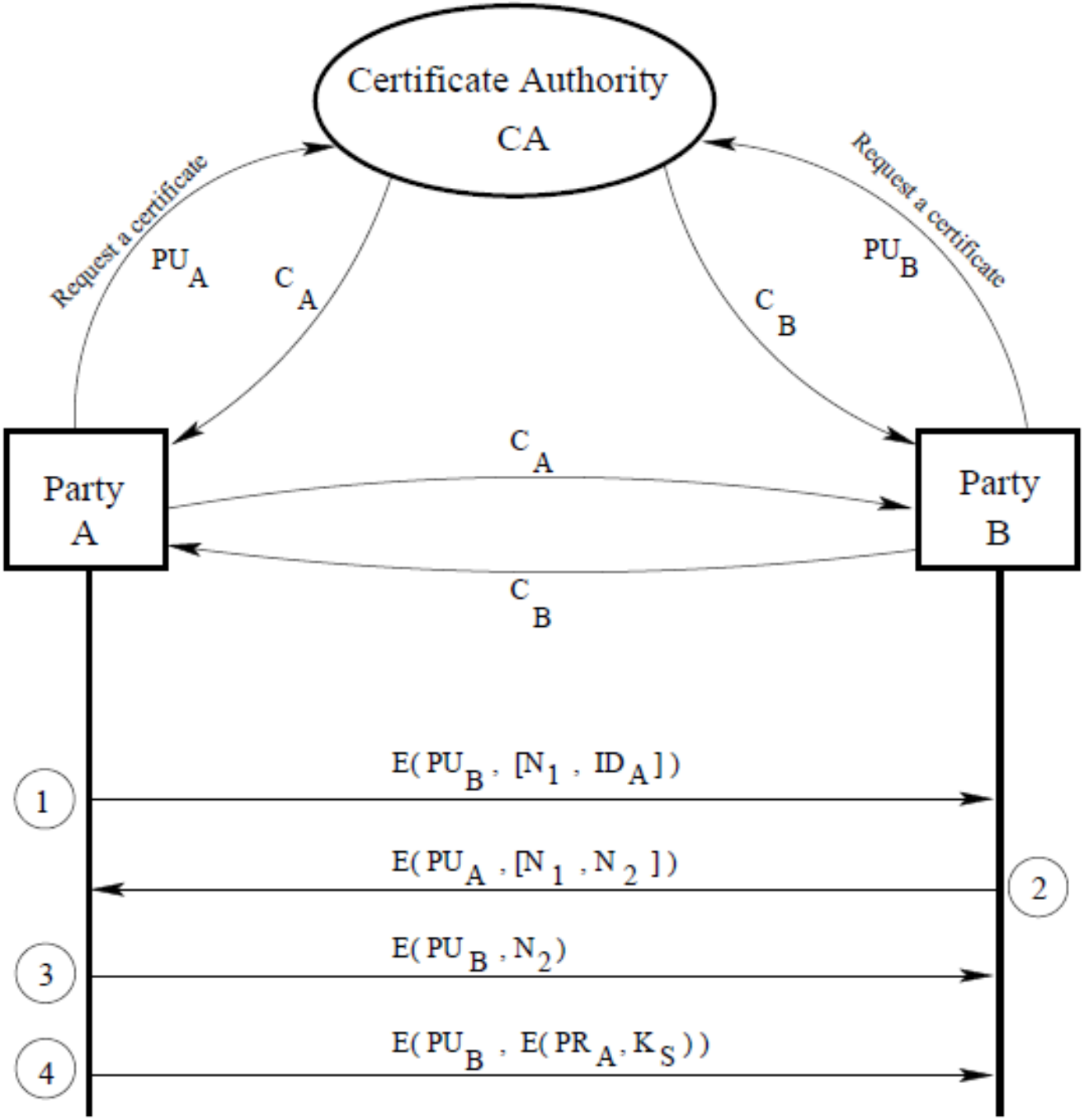
Les certificats des clés révoquées doivent alors être mises dans une **liste des certificats révoqués** (CRL : *Certificate Revocation List*)

La fin de vie d'une clé

Lorsqu'une clé arrive en fin de vie (crypto-période), il convient de créer et d'échanger une nouvelle clé pour remplacer l'ancienne

Il est tout à fait déconseillé d'utiliser l'ancienne clé pour transmettre la nouvelle clé confidentiellement


user registration
KEY STATE
user initialization
new user
key generation
key establishment protocol
pre-operational
recovered key
initial key
existing user
key recovery
key installation
new key
key update
new key
key backup
key loss without compromise
key registration
public key directory
operational
normal use of key
key compromise or early termination
cryptoperiod expiry
old key (expired)
revocation
archival
post-operational
key movement
system trigger
key de-registration and destruction
obsolete


Certificate Authority
CA
Request a certificate
PU A
C A
Request a certificate
PU B
C B
Party A
Party B
C A
C B
1
E(PU B , [N 1 , ID A])
2
E(PU A , [N 1 , N 2])
3
E(PU B , N 2)
4
E(PU B , E(PR A , K S))