Chiffrement Asymétrique

Partie 2

Dr. Noureddine Chikouche
noureddine.chikouche@univ-msila.dz
https://sites.google.com/view/chikouchenoureddine

Plan du cours

- Echange de clés
- Protocole d'échange de clés RSA
- Protocole de Diffie-Hellman
- Comparaison

Echange de clés

- Les protocoles d'Internet utilisent largement les clés de session.
- Une clé de session (*session key*) est une clé symétrique temporaire utilisée pour protéger les données transmis par les chiffrent pendant une session de communication.

Echange de clés

- Pour échanger des clés de session (symétriques), on peut utiliser deux moyens:
  - Canal sécurisé: rarement disponible.
  - Canal non sécurisé (public): Internet, Wifi, mobiles, …
- Les algorithmes à clé publique (comme RSA) n'est pas utilisé pour le chiffrement des données, mais plutôt pour l'échange de clés de session pour la cryptographie symétrique.

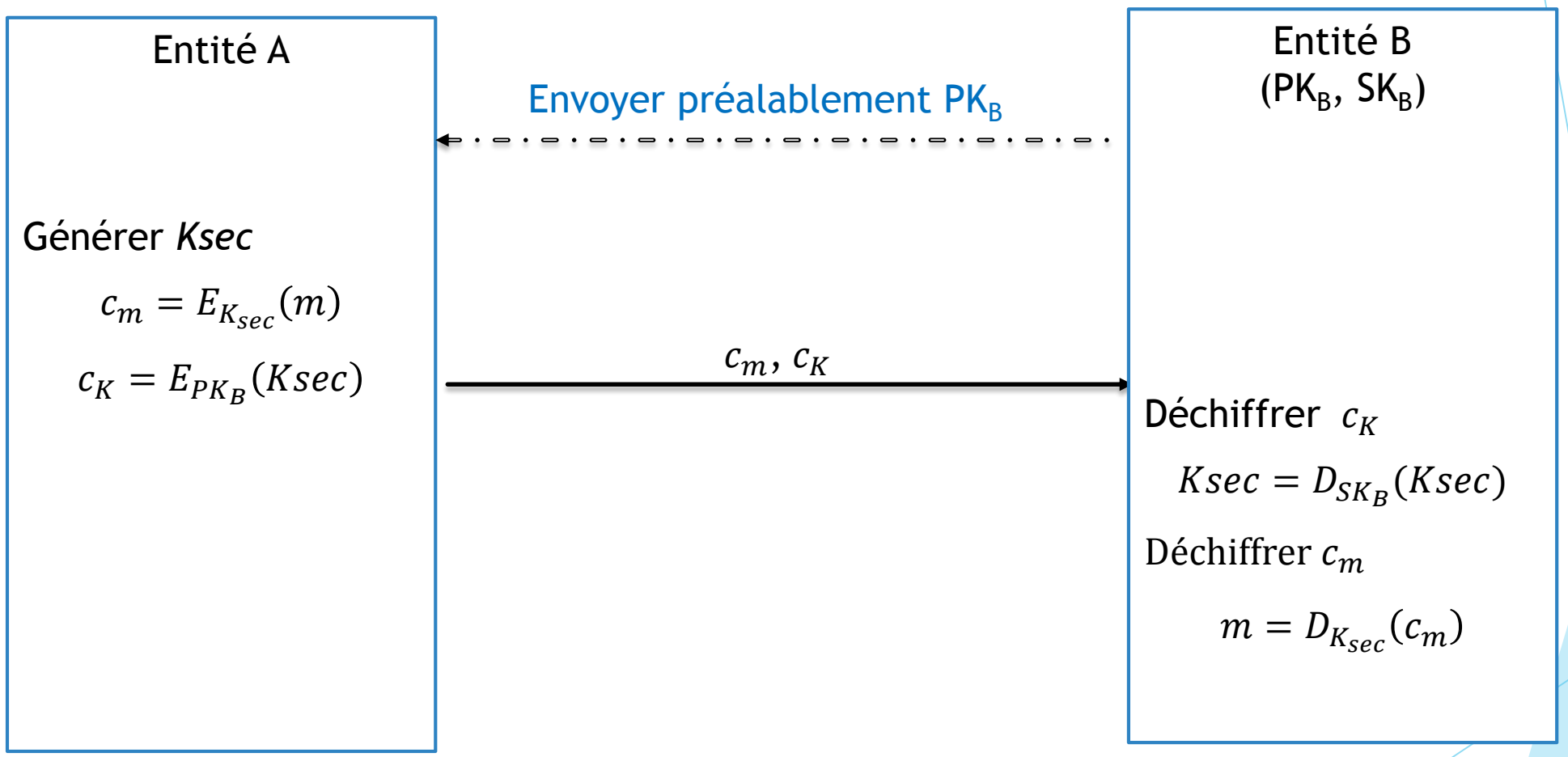
Echange de clés

- Pour échanger de clés, on utilise les protocoles d'échange de clés.
- Il existe deux catégories de protocoles d'échange de clés:
  - Utiliser des connaissances partagées préalablement entre les entités communicants. Par exemples, protocole d'échange de clés RSA.
  - Ne pas Utiliser des connaissances partagées préalablement entre les entités communicants. Par exemple, protocole d'échange de clé Diffie-Hellman.

Protocole d’échange de clés RSA

- L’information préalablement échanger entre les entités est la clé publique de destinataire.
- Ce protocole utilisé par le protocole HTTPS et PGP.
- On utilise le principe de chiffrement hybride:
  - Chiffrer la clé session par la clé publique de destinataire.
  - Chiffrer le message à envoyer par la clé de session (chiffrement symétrique).

Protocole d'échange de clés RSA

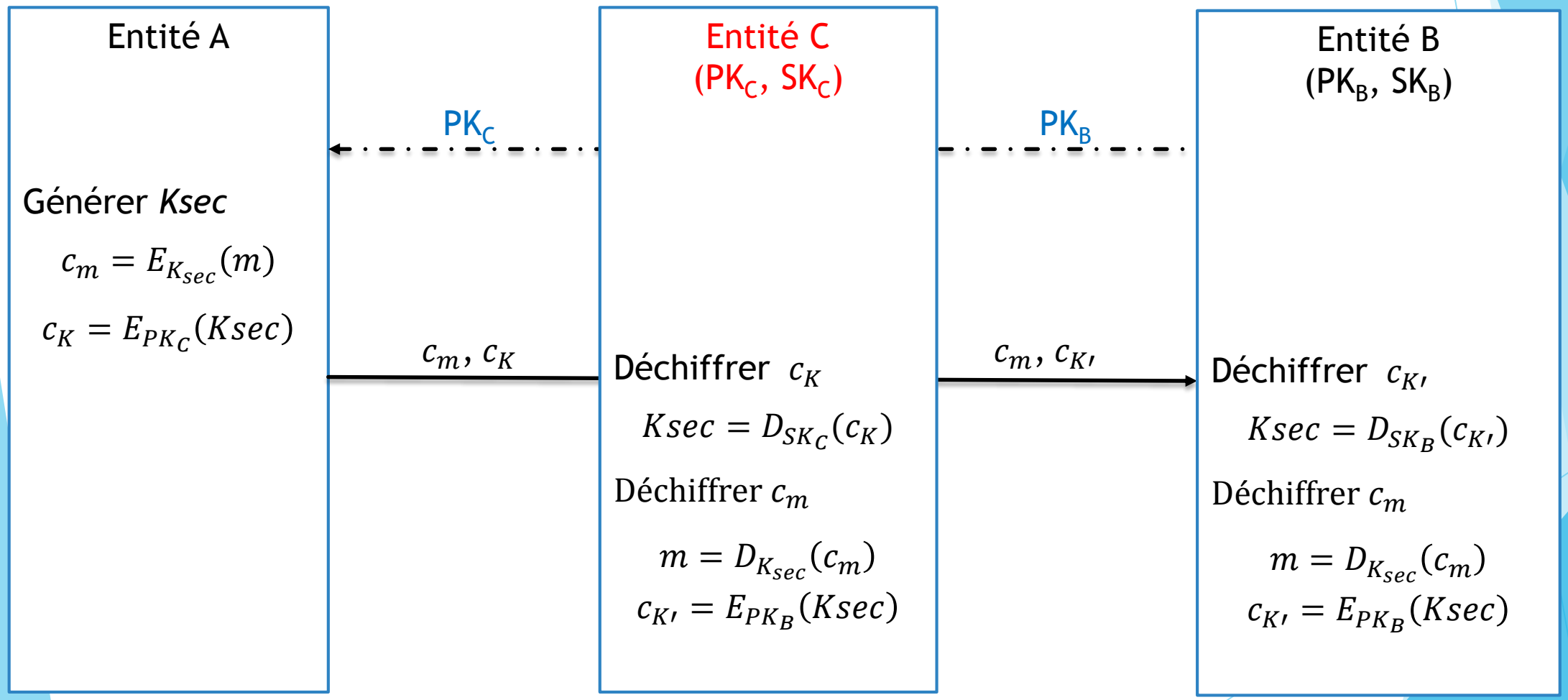


Protocole d'échange de clés RSA

- L'entité A choisit aléatoirement une clé de session *Ksec* (*ex.* de taille 128 bits pour AES-128).
- A chiffre le message à envoyer par la clé $Ksec$ en utilisant la fonction de chiffrement symétrique, $c_m = E_{K_{sec}}(m)$
- A chiffre la clé de session par la clé publique de destinataire (PK_B), $c_K = E_{PK_B}(Ksec)$
- A envoie c_m et c_K à l'entité B.
- B déchiffre c_K avec sa clé privée pour obtenir le clé session $Ksec = D_{SK_B}(Ksec)$
- B déchiffre le message chiffré par la clé de session reçue, $m = D_{K_{sec}}(c_m)$.

Protocole d'échange de clés RSA

Attaque



Protocole d'échange de clés RSA
Attaque

- Le protocole d'échange de clés RSA est vulnérable aux attaques actives «par milieu» (*man-in-the-middle*).
- Principe d'attaque:
  - Lors d'échange de la clé publique de *B*, l'attaquant *C* remplace PK_B par sa clé publique (PK_C) et l'envoie à *A*.
  - L'entité *A* utilise la clé publique de *C* pour chiffrer la clé de session. Alors, l'attaquant peut obtenir tout simplement la clé de session pendant la communication entre A et B.
- Pour éviter cette vulnérabilité, il faut certifier la clé publique de destinataire.

Protocole de Diffie Hellman

Diffie & Hellman

- Premier schéma de clé publique proposé en 1976.

Protocole de Diffie et Hellman

- Ce protocole est plus utilisé pour l'échange d'une clé secrète (ou de session) sans besoin des informations préalablement partagée.
- Il est souvent utilisée dans des produits commerciaux (SSL,...).
- Non authentifié dans la version de base.
- La sécurité du protocole DH repose sur le problème Logarithme discret et sur le problème de DH.

Protocole de Diffie Hellman

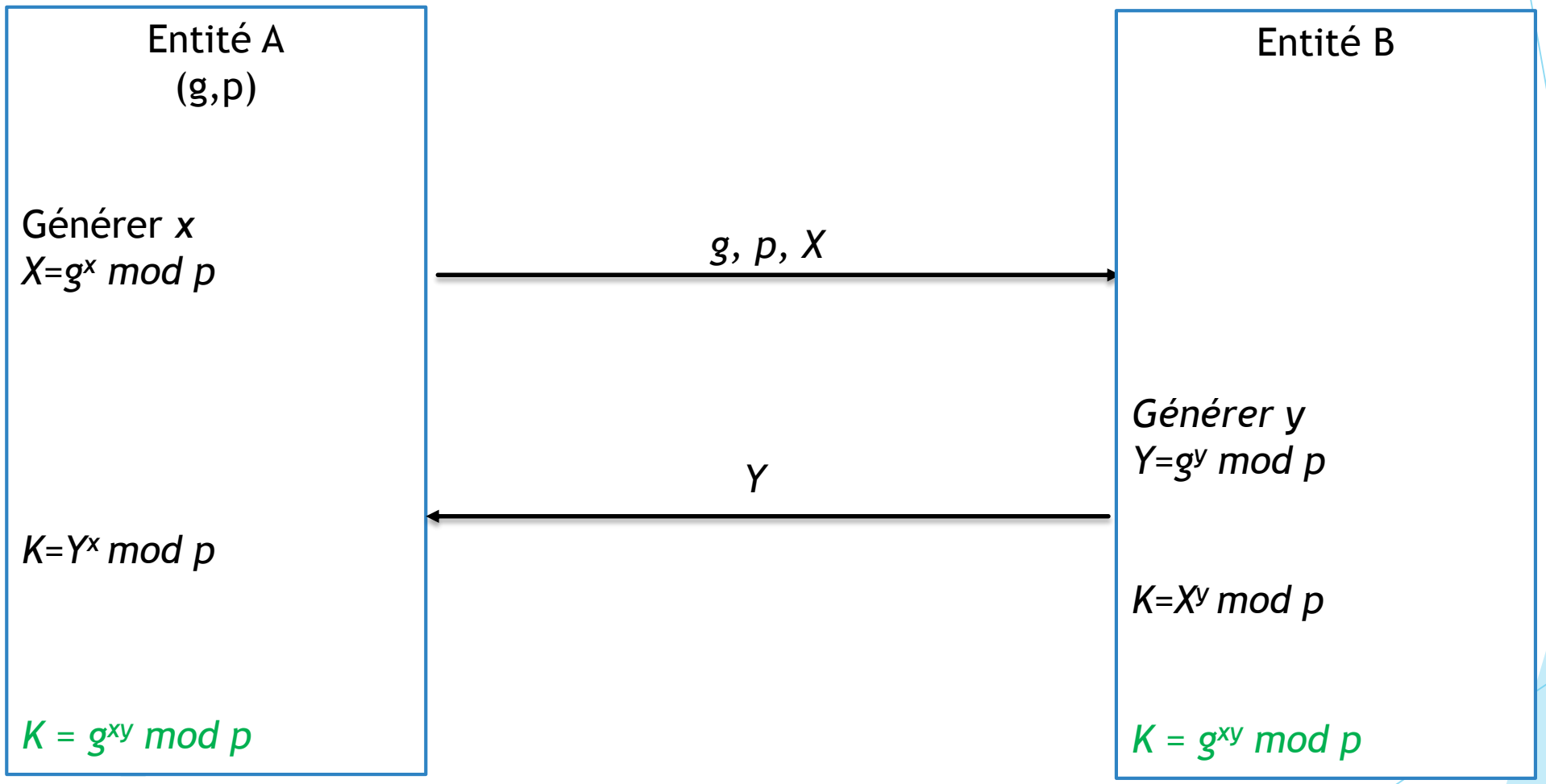
Logarithme discret

- Soit G un groupe cyclique. Soient p un grand premier et g un générateur de $\mathbb{Z}_p^*$.
- Etant donné x, calculer $y = g^x \bmod p$ se fait facilement par exponentiation rapide.
- Problème: Trouver $x = \log_g(y) \bmod p-1$. Connaissant y, g et p.
- **Applications:** cryptosystème El-Gamal et protocole de Diffie-Hellman.

Protocole Diffie et Hellman version de base

- Le problème de DH signifie la difficulté de calcul de $k = g^{xy} \bmod p$ à partir de $X=g^x \bmod p$ et de $Y=g^y \bmod p$, lorsque p est grand.
- x et y sont des clés privées.
- X et Y sont des clés publiques.

Protocole Diffie et Hellman version de base



Protocole Diffie et Hellman version de base

- Soit p un grand nombre premier et g un générateur de Z_p^*.
- A choisi un entier x et calcule $X=g^x \bmod p$.
- A envoi X, g, et p à B.
- B choisit un entier y et calcule $Y=g^y \bmod p$.
- B envoie Y à A.

Protocole Diffie et Hellman version de base

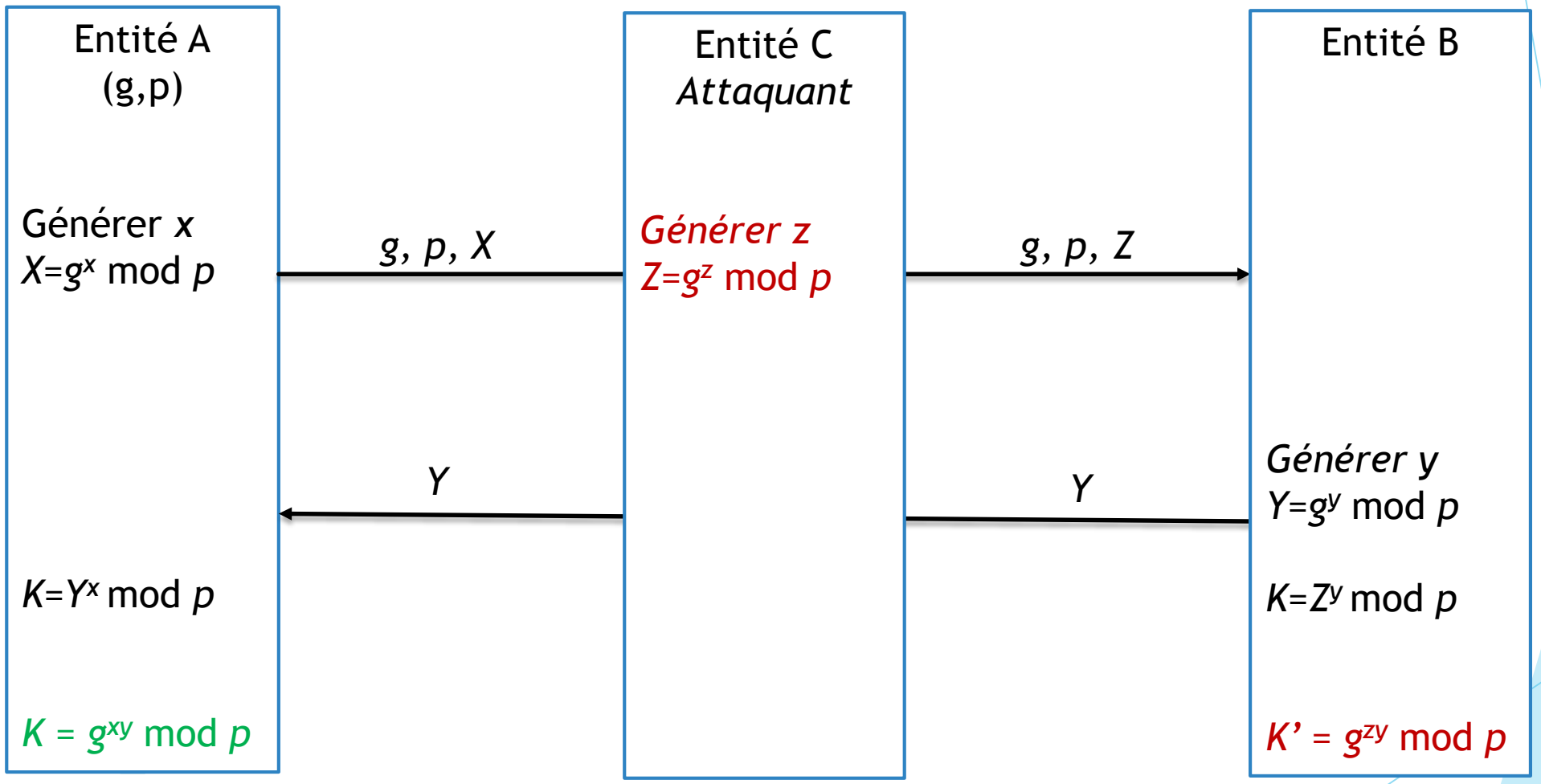
- L'entité A calcule $(g^y \bmod p)^x \bmod p = g^{xy} \bmod p$
- L'entité B calcule $(g^x \bmod p)^y \bmod p = g^{xy} \bmod p$
- La clé secrète partagée est:

$$K = g^{xy} \bmod p$$

Protocole Diffie et Hellman version de base

- **Exemple:**
- On Suppose que les entités A et B partagent p = 233 et g = 45 :
- A choisit ***x*** = 11 et Bob y = 20, alors
  - X = 45^{11} mod 233 = 147,
  - Y = 45^{20} mod 233 = 195,
- Y^x mod p = 195^{11} mod 233 = 169
- X^y mod p = 147^{20} mod 233 = 169.
- Les entités A et B disposent d'une clé secrète partagée, k = 169.

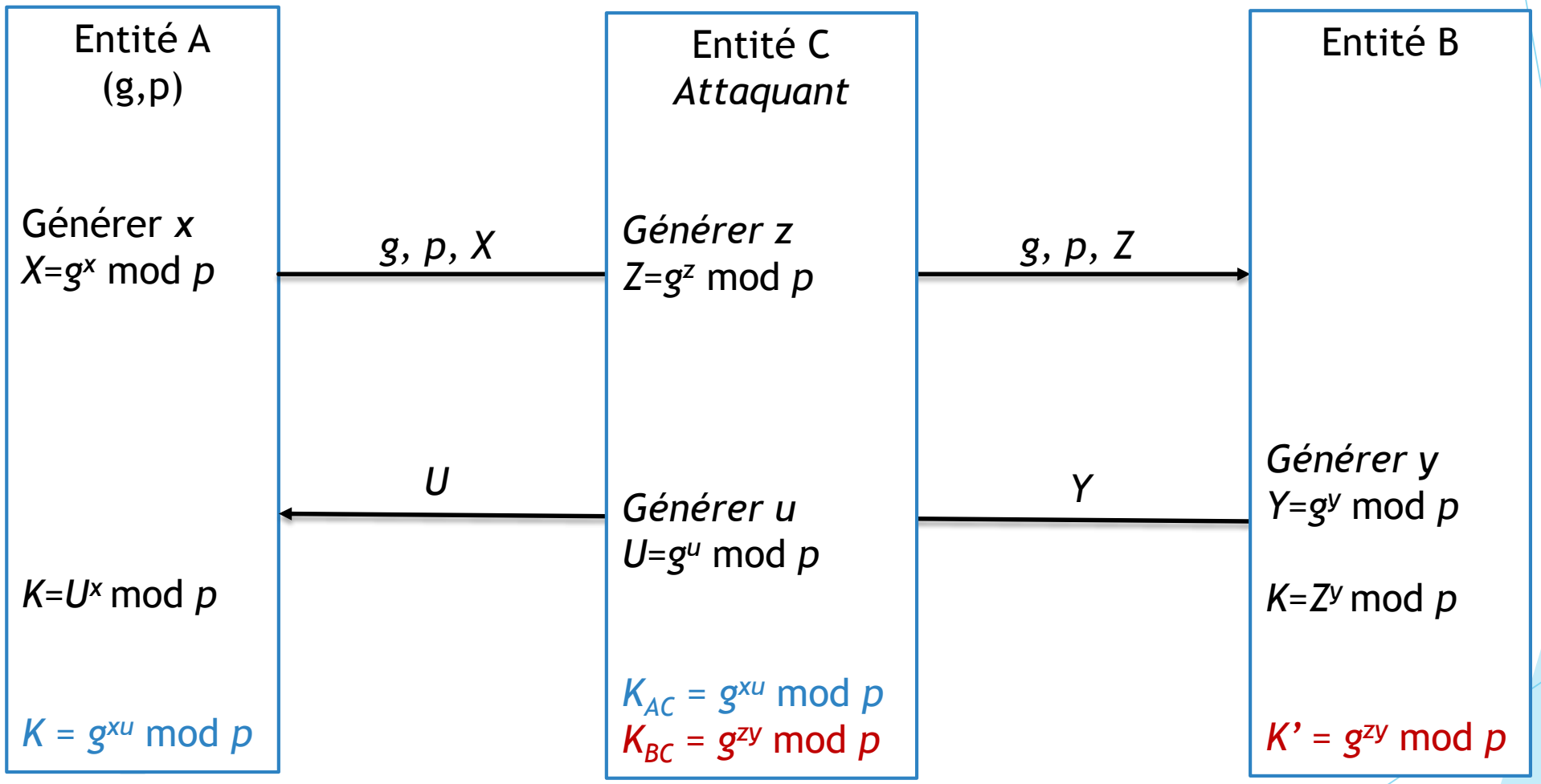
Protocole Diffie et Hellman
Attaque 1



Protocole Diffie et Hellman
Attaque 1

- Le protocole DH est vulnérable aux attaques actives « par milieu» (*man-in-the-middle*).
- Lors de l'échange des clés, l'attaquant *C* bloque le message X envoyé par A, sélectionne un nombre aléatoire *z* et calcule $Z = g^z \bmod p$. C envoie le message Z à l'entité B.
- Résultat: les deux entités A et B calculent deux clés différentes, $k_A = g^{xy} \bmod p$ pour l'entité A et $k_B = g^{yz} \bmod p$ pour l'entité B.
- Lorsque l'entité A envoie un message chiffré *m* en utilisant sa clé secrète, l'entité B ne peut pas obtenir le message clair de A.

Protocole Diffie et Hellman
Attaque 2



Protocole Diffie et Hellman
Attaque 2

- Le protocole DH est vulnérable aux attaques actives « par milieu» (*man-in-the-middle*):
- Lors de l'échange des clés, l'attaquant *C* modifie les messages envoyés *X* et *Y et les remplace par des nouveaux messages Z et U*, respectivement.
- Les entités A et B crée des clés de session différentes, K et K'.
- L'attaquant crée de clés K_{AC} et K_{BC}, tels que: $K_{AC} = K$ et $K_{BC}=K'$.

Protocole Diffie et Hellman
Attaque 2

- Lorsque *A* envoie un message chiffré $E_K(m)$ à *B*, l'attaquant intercepte le message envoyé, puis le déchiffre en utilisant la même clé K_{AC}.
- Cependant, l'entité B ne peut pas obtenir le message clair à cause de *K* et *K'* sont différentes.
- L'attaquant *C* peut appliquer le même scénario avec B.

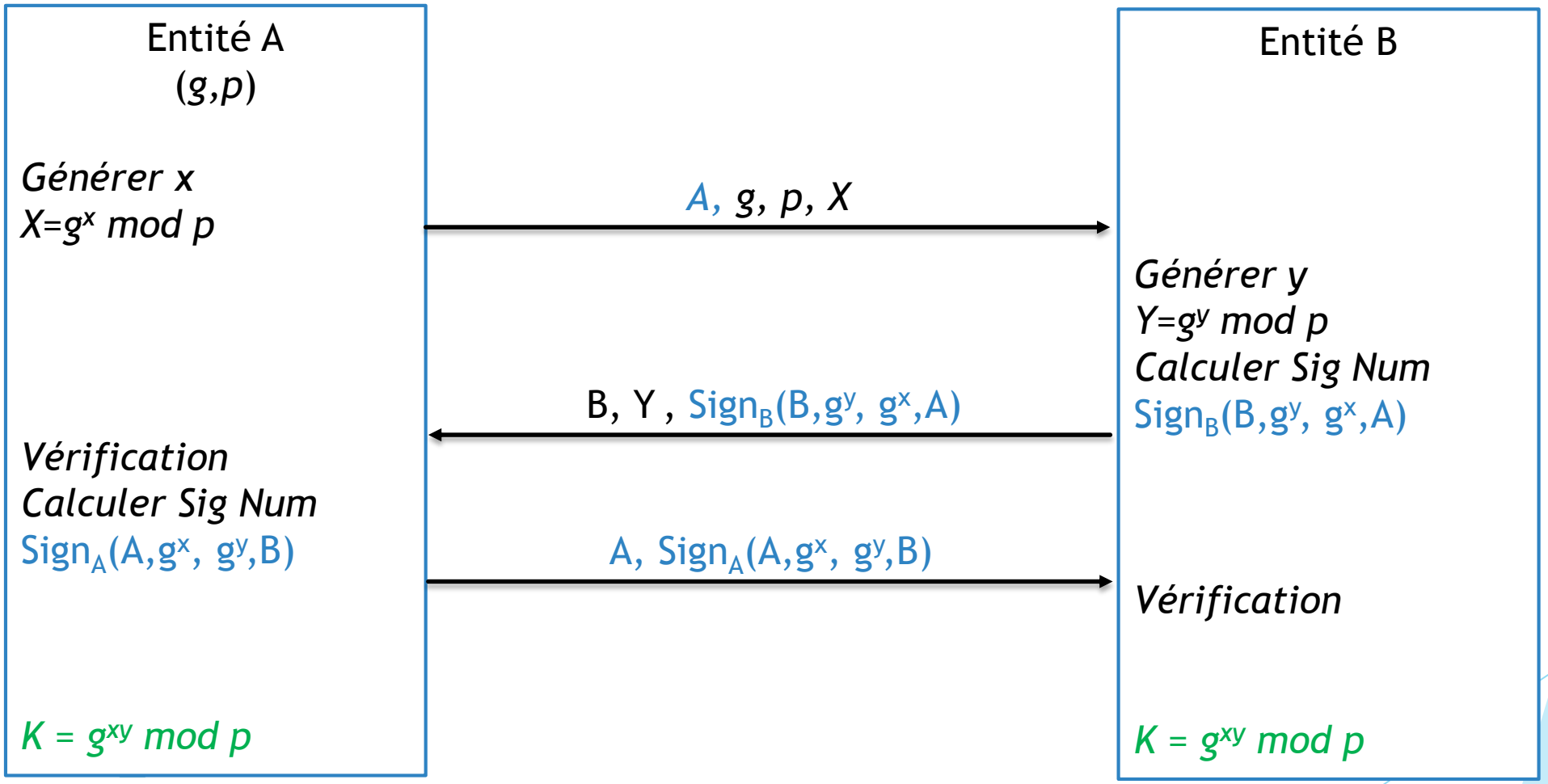
Protocole Diffie et Hellman
Avantages & Inconvénient

- Avantages:
  - Problème de Logarithme discret est dur.
- Inconvénients:
  - Un attaquant peut observer: p, g $g^b \mod p$ et $g^a \mod p$
  - Comme RSA, très lent.
  - Pas d'authentification

Protocole Diffie et Hellman version signée

- Afin d'éviter l'attaque par milieu, la solution est d'utiliser la signature numérique.
- Elle consiste à ce que:
  - l'entité A envoie (A, g^x),
  - B envoie $(B, g^y, Sign_B(B, g^y, g^x, A))$
  - A vérifie la signature reçue et calcule la clé secrète ***K***.
  - Enfin A calcule sa signature $(A, Sign_A(A, g^x, g^y, B))$ et l'envoie à B.
  - B vérifie la signature reçue et calcule la clé secrète ***K***.

Protocole Diffie et Hellman version signée



Comparaison

Chiffrement symétrique vs Chiffrement asymétrique

	Symétrique	Asymétrique
Avantages	• Il est plus rapide en exécution et nécessite moins de puissance de calcul. • Il utilise des petites clés (64 – 256) bits. • Il est implémenté sur le hardware facilement.	• Permettre de signer des messages. • Faciliter de distribution des clés. • Il nécessite 2*n* clés seulement pour *n* entités communicants.
Inconvénients	• Il ne fournit pas certaines services (ex. signature). • Distribution des clés. • Il nécessite *n(n-1)/2* clés pour *n* entités communicants.	• Il est lent à l'exécution (1000 fois plus lents). • Taille de clé largement augmentée.

Ressources

- P. Boyer, cryptographie, 2013, http://www.math.univ-paris13.fr/boyer/enseignement/images.html
- Cryptographie à clé publique, MGR850, École de technologie supérieure (ÉTS). https://cours.etsmtl.ca/mgr850/documents/cours/MGR850_A14_Cours-06_cryptoAsym.pdf