WEP - Wired Equivalent Privacy

- Le standard 802.11 intègre un mécanisme simple de chiffrement des données, il s'agit du WEP, *Wired Equivalent Privacy, en* se basent sur un l'algorithme à clé symétrique RC4.
- Cette clé est partagée par tous les clients du réseau et par le point d'accès à 40 ou 104 bits (5 ou 13 caractères ASCII/ 10 ou 26 caractères hexa).
- L'utilisation du WEP est précisée dans le champ FC (Frame Control) de la trame de données.
- Ce protocole répond aux trois principes fondamentaux de sécurité:
  - ✓ authentification
  - ✓ confidentialité des données
  - ✓ intégrité des données.

Authentification

- Le mécanisme d'authentification utilise la clé partagée pour l'envoi des données chiffrées. Il existe deux mécanismes d'authentification :

  - Open System Authentication : mécanisme par défaut, il n'y a pas d'authentification véritable, toute station désirant se connecter, est automatiquement authentifiée.

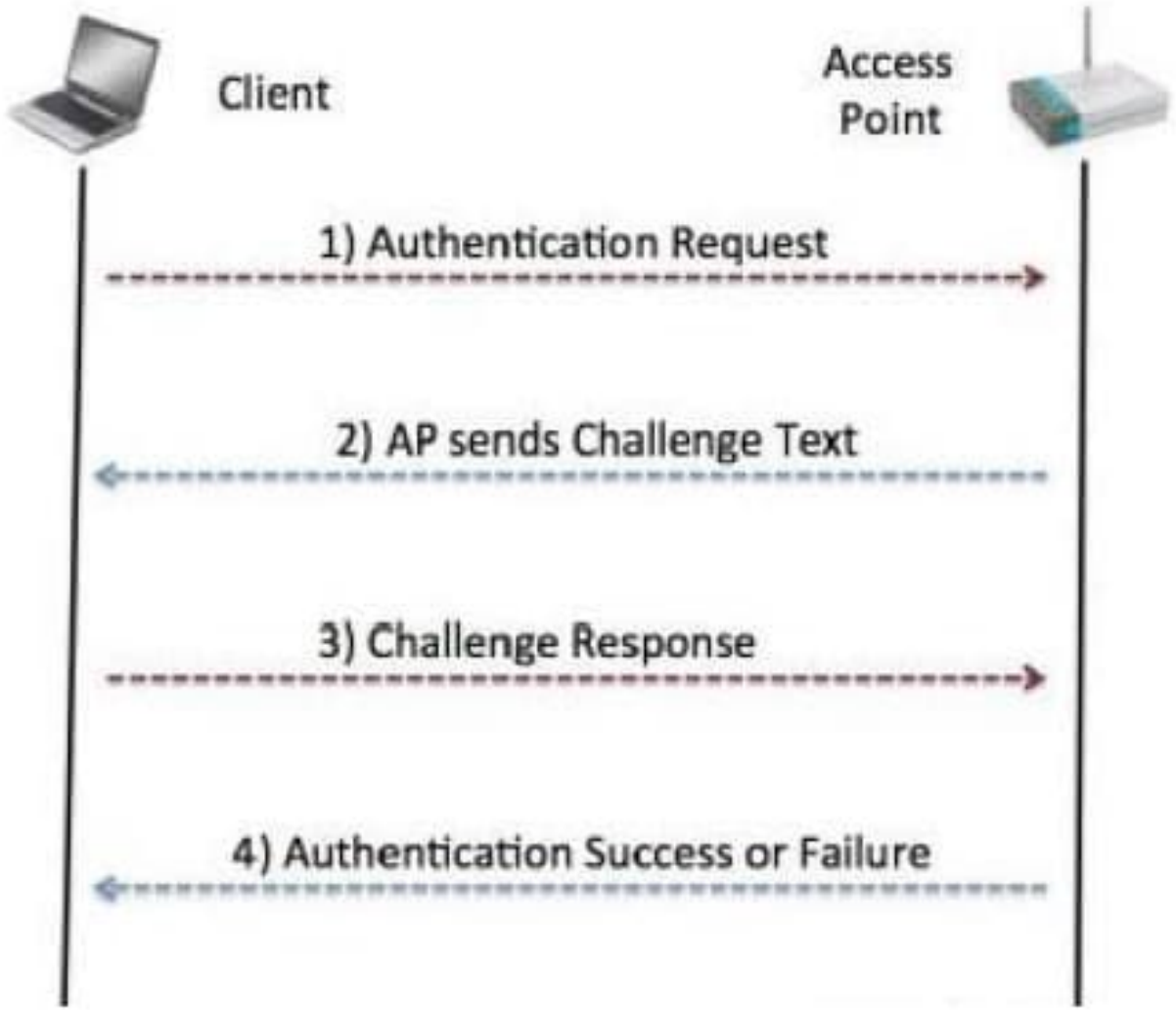
  - Shared Key Authentication : ce mécanisme se déroule en quatre étapes :

    ① La station envoie une requête d'authentification au point d'accès.

    ② Le PA envoie un texte en clair 128 bits généré par l'algorithme WEP

    ③ La station chiffre ce texte avec la clé partagée et l'envoie dans une trame d'authentification.

    ④ Le PA déchiffre le texte reçu avec la même clé partagée et le compare avec le texte précédent, s'il y a égalité il confirme à la station son authentification et la station peut alors s'associer. Sinon le PA envoie une trame d'authentification négative.



Distribution de clé

- Peut être choisie sous forme hexadécimale ou ASCII.
- Elle doit être saisie manuellement sur les postes des clients.
- Caractères ASCII → bits de poids forts sont nuls → clés vulnérables.
- Il est recommandé de choisir des passphrases de 104 bits.
- La clé est stockée sur des fichiers en clair → il est recommandé de changer fréquemment de clé.
- Possibilité de configurer l'AP et les clients à utiliser plusieurs clés (4).

WEP: Objectifs de départ

- Raisonnablement fort: la sécurité de base sur la difficulté de trouver la clé secrète.
- Efficace: peu consommable de point de vue ressources (puissance de calcul+ énergie)
- Optionnel.

WEP « essaie » d'assurer:

- L'authentification
- Le confidentialité par un chiffrement RC4
- L'intégrité

MAIS il s'avère que tous ces services sont facilement contournables!

Chiffrement et contrôle d'intégrité

- Basé sur l'algorithme RC4, développé par Ron Rivest en 1987 pour RSA Security.
- Le chiffrement et le contrôle d'intégrité se déroulent en plusieurs étapes:

① La création de la graine *(seed)*,
② La création du keystream,
③ Le calcul ICV *(Integrity Check Value)*,
④ La constitution du message final et son encapsulation dans une trame.

Création de la graine

- Un Vecteur d'initialisation (*IV*) est une séquence de bits qui change régulièrement à chaque trame envoyée. Combiné à la clé statique *K*, il introduit une notion aléatoire au chiffrement.
- La longueur du IV est de 24 bits, soit 2^{24} valeurs possibles.
- Le IV doit être connu à la fois de l'émetteur et du récepteur → il est donc transporté en clair dans les trames.

Initialisation de la clé

- Deux longueurs de clé WEP peuvent être choisies sur les équipements Wi-Fi : 40 bits ou 104 bits.
- On obtient une graine (*seed*) de 64 bits (ou 128 bits) en concaténant le IV à la clé :

$$seed = IV \,||\, K$$

Création de la graine (2)

Clé d'origine:

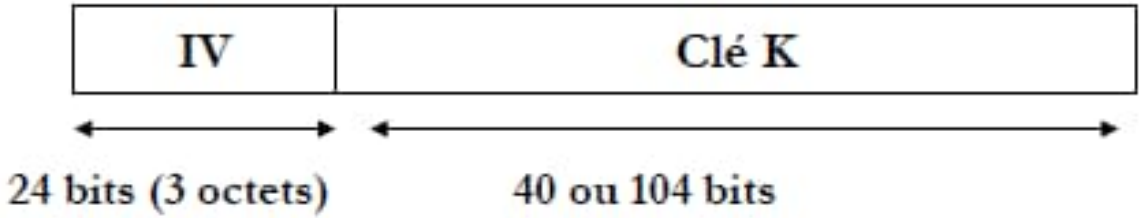
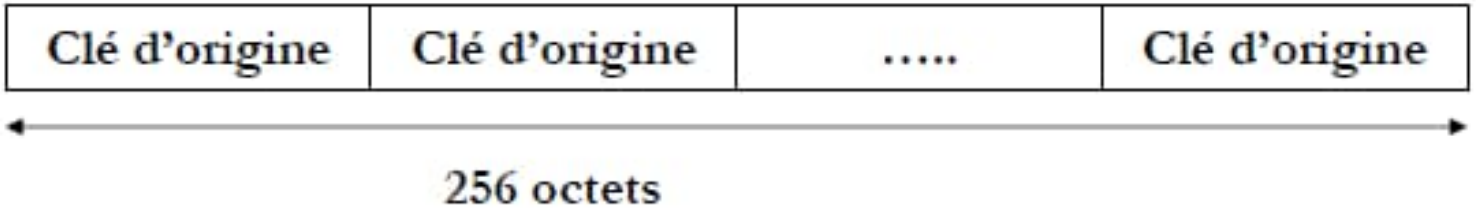


Table d'initialisation:

Une table d'états T est créée et mélangée.



Ce procédé porte le nom de *Key Scheduling Algorithm* (KSA) ou encore module de mise à la clé.

Obtention du keystream:

- Une fois la table T mélangée, on peut fabriquer des PRNs ou « Pseudo Random Numbers » à l'aide d'un générateur PRGA ou « Pseudo Random Generator Algorithm ».
- La clé de chiffrement utilisée est une séquence de bits extraite de cette table à partir du PRGA. On appelle cette séquence masque ou encore keystream (sortie RC4).

$$\text{KeyStream} = \text{PRNG}(IV||K)$$
$$= \text{RC4}(IV||K)$$

Le calcul du ICV

- On effectue, avec un CRC 32 (*Cyclic Redundancy Check*), un calcul d'intégrité (non chiffré) ou ICV (Integrity Check Value) sur les données.
- Les données sont, ensuite, concaténées avec cet ICV.

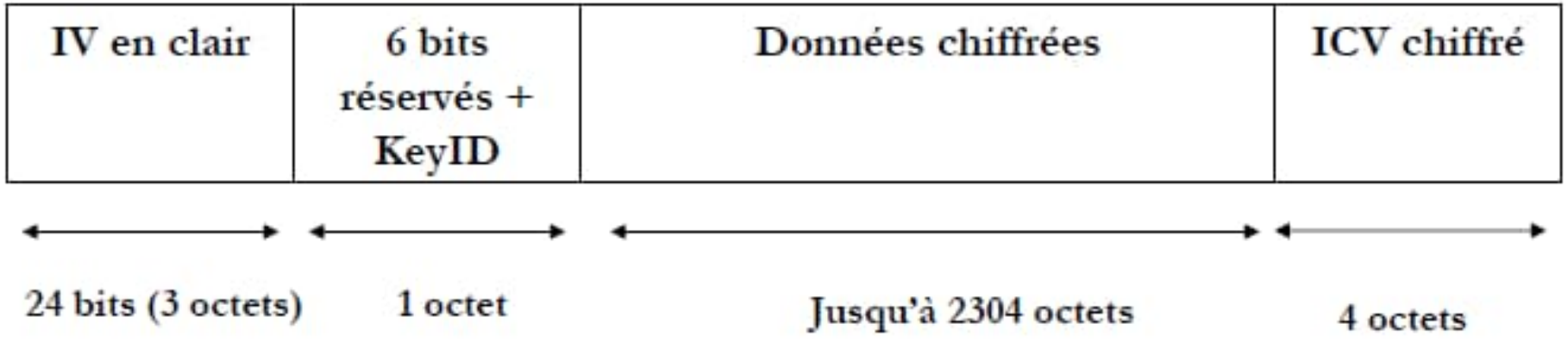
Payload = [Data| |ICV]

Encapsulation du message final dans une trame

- On réalise un XOR (OU exclusif ou addition modulo 2) bit à bit entre la KeyStream générée précédemment et le payload.

$$\text{Cryptogramme} = (M||ICV(M)) \text{ xor } RC4(IV||K)$$

- La trame à envoyer sera donc : IV || C



Déchiffrement et contrôle d'intégrité

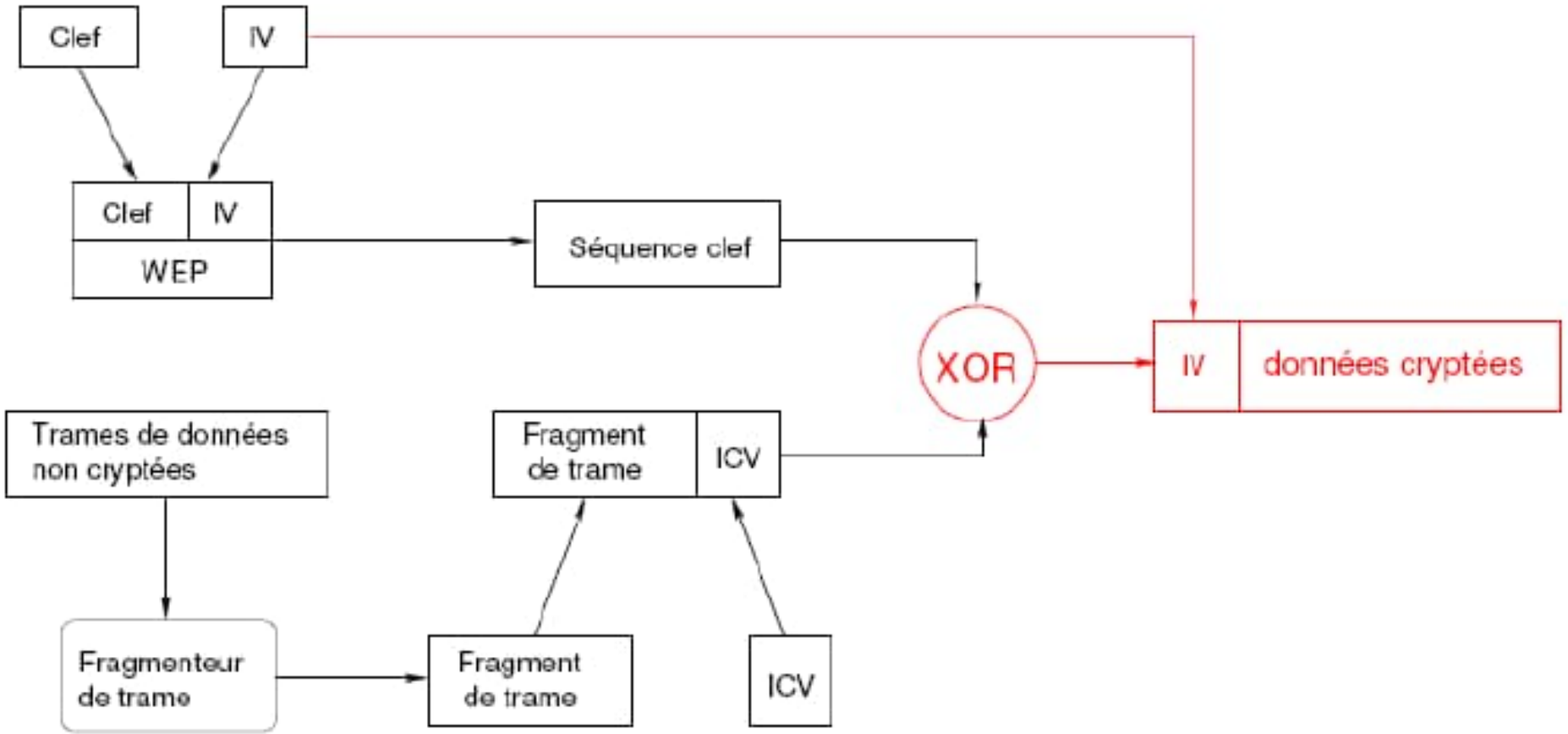
Le déchiffrement et le contrôle d'intégrité se déroulent en plusieurs étapes comme précédemment, mais en sens inverse :

① La clé partagée est concaténée avec l'IV de la trame reçue, puis l'ensemble est introduit dans le PRNG pour donner la bonne séquence pseudo aléatoire qui a été utilisé pour le chiffrement.

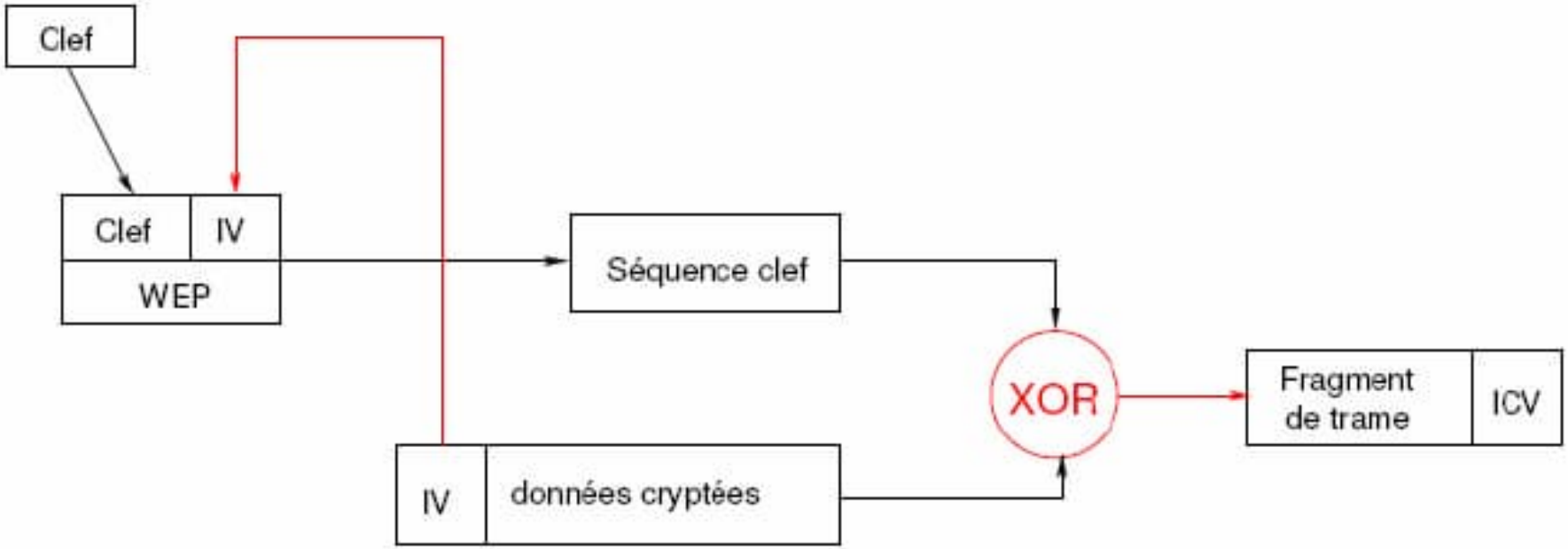
② On effectue un XOR entre cette séquence aléatoire et les données chiffrées reçues. On obtient les données et l'ICV en clair.

③ On effectue un contrôle (ICV') sur ces données en clair que l'on compare avec l'ICV reçu. Si ICV'=ICV on peut être sûr des données.

Chiffrement (schéma complet)



Déchiffrement (schéma complet)



Les failles du WEP

Faiblesses conceptuelles dans:

- L'authentification
- Le contrôle d'intégrité
- Le chiffrement
- La gestion de clé

Les failles du WEP

Mécanisme d'authentification inefficace

- Acquisition de la clé WEP soit par une *ingénierie sociale* soit par une *cryptanalyse*.
- La clé WEP est très courte (40 ou 104 bits), → Attaque par force brute.
- Ecoute du Challenge text et son cryptogramme pendant l'authentification.
- Un AP malicieux peut envoyer des challenges à chiffrer aux stations du réseau qui deviennent des oracles *(Man in The Middle)*.

Faible contrôle d'intégrité

- A cause de la linéarité du CRC, il est possible d'injecter des trames forgées valides servant à déjouer l'authentification, à procéder à une attaque texte clair connu (sur un réseau Ethernet) ou à réaliser du spoofing (attaque par mascarade) (Cf TD).

Les failles du WEP (2)

Problèmes de rejeu de keystream

- L'IV circule en clair.
- Théorème des anniversaires : la probabilité d'avoir deux trames chiffrées avec le même IV (collision de clé) est à 99% de chance pour se produire après 12000 trames!

  - ⇨ Possibilité de construire des dictionnaires en rejouant le keystream : détecter les collisions de clé par une simple écoute d'un trafic assez volumineux (en récupérant la sortie RC4 de longueur 64 ou 128 bits).
  - ⇨ Déchiffrer des morceaux de trames chiffrées avec le même IV.
  - ⇨ Injecter des paquets (ARP ou HTTP) valides contenant des attaques de niveau supérieur.

(Cf TD)

Les failles du WEP (3)

Problème de clé faible

- L'IV circule en clair: on peut donc reconnaître les clés faibles à partir de leurs premiers octets.
  - Repérer par une écoute du trafic les trames chiffrées avec des clés faibles et procéder à une attaque du RC4.
  - Attaques FMS (Fluhrer, Mantin et Shamir) dans Aireplay et Aircrack.

Problème de clé statique et partagée

Même clé pour l'authentification et le cryptage!

WEP : Weak Encryption Protocol ?

Les failles du WEP (4)

- Le WEP est limité aux réseaux de petite taille, de moindre trafic.
- Modification régulière de clé.
- Association avec d'autres mécanismes (IPSec, SSL,…)
- Le WEP existe toujours pour assurer une rétro-compatibilité de matériels.