Introduction à la cryptographie – Chapitre IV

Exemple

Plan du cours

- 0. Courte introduction.
- I. Systèmes à clef publique.
- II. Systèmes à clef secrète.
- III. Authentification.
- IV. Exemples.

Plan du cours

- 0. Courte introduction.
- I. Systèmes à clef publique.
- II. Systèmes à clef secrète.
- III. Authentification.
- IV. Exemples.

- **4.1. Bluetooth.**
- **4.2. Wifi.**
- **4.3. Wimax.**
- **4.4. GSM.**
- **4.5. UMTS.**
- **4.6. SSL / TLS.**
- **4.7. Carte vitale.**
- **4.8. Carte bancaire.**

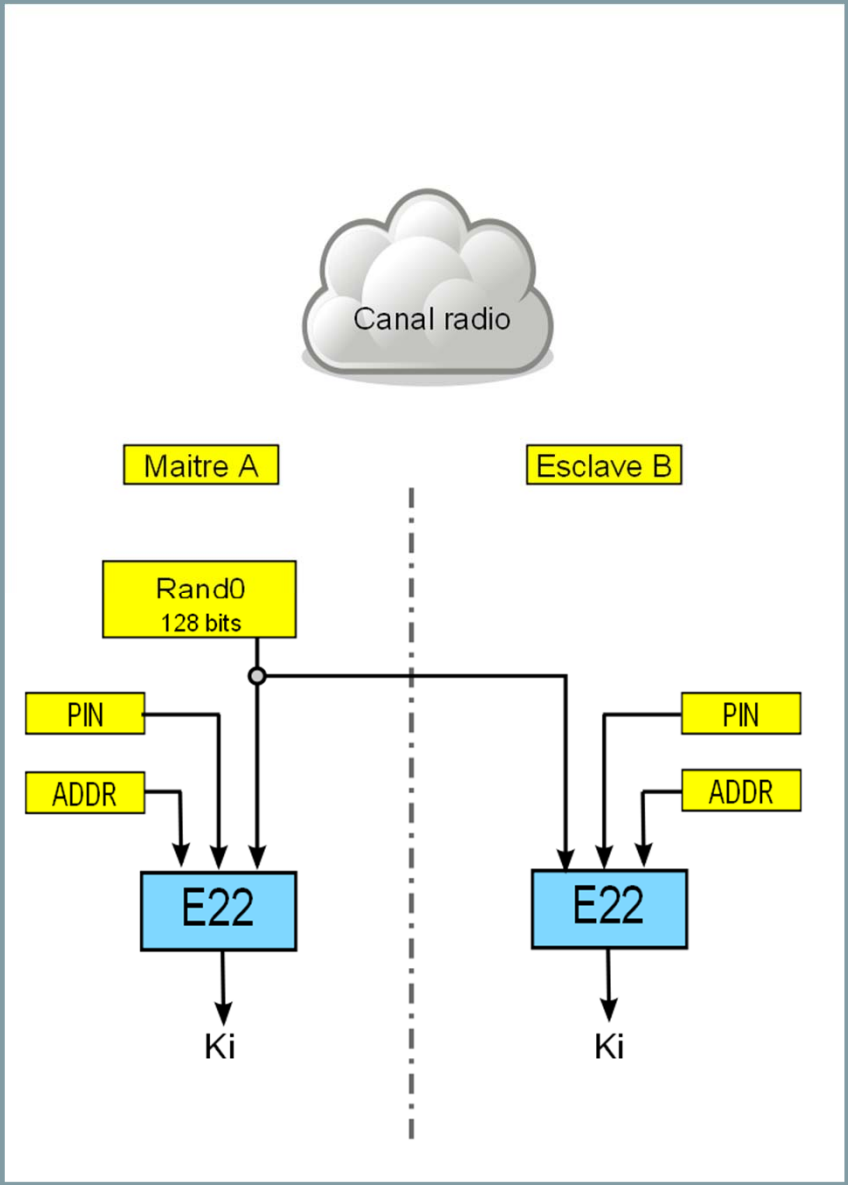
- Il existe différents types de clefs dans Bluetooth.
- La clef de lien est un nombre aléatoire de 128 bits utilisé dans la procédure d'authentification. Elle sert ensuite à construire la clef de chiffrement.
- Le code PIN sert à authentifier l'utilisateur. Sa taille varie de 1 à 16 octets.
- Il existe trois modes de sécurité différents :
  - Mode non sécurisé.
  - Mode sécurisé au niveau de la couche de service.
  - Mode sécurisé au niveau de la couche de liaison.

- Le pairage est l'établissement d'un canal sécurisé dans le mode 3. Il comprend trois étapes :
  - Création d'une clef d'initialisation.
  - Création d'une clef de lien.
  - Authentification mutuelle.
- Une fois ces trois étapes effectuées, les appareils partagent une clef de chiffrement commune qui leur permet d'assurer la confidentialité des communications.
- Nous allons détailler les étapes et décrire les algorithmes.

Clef d'initialisation. (1)

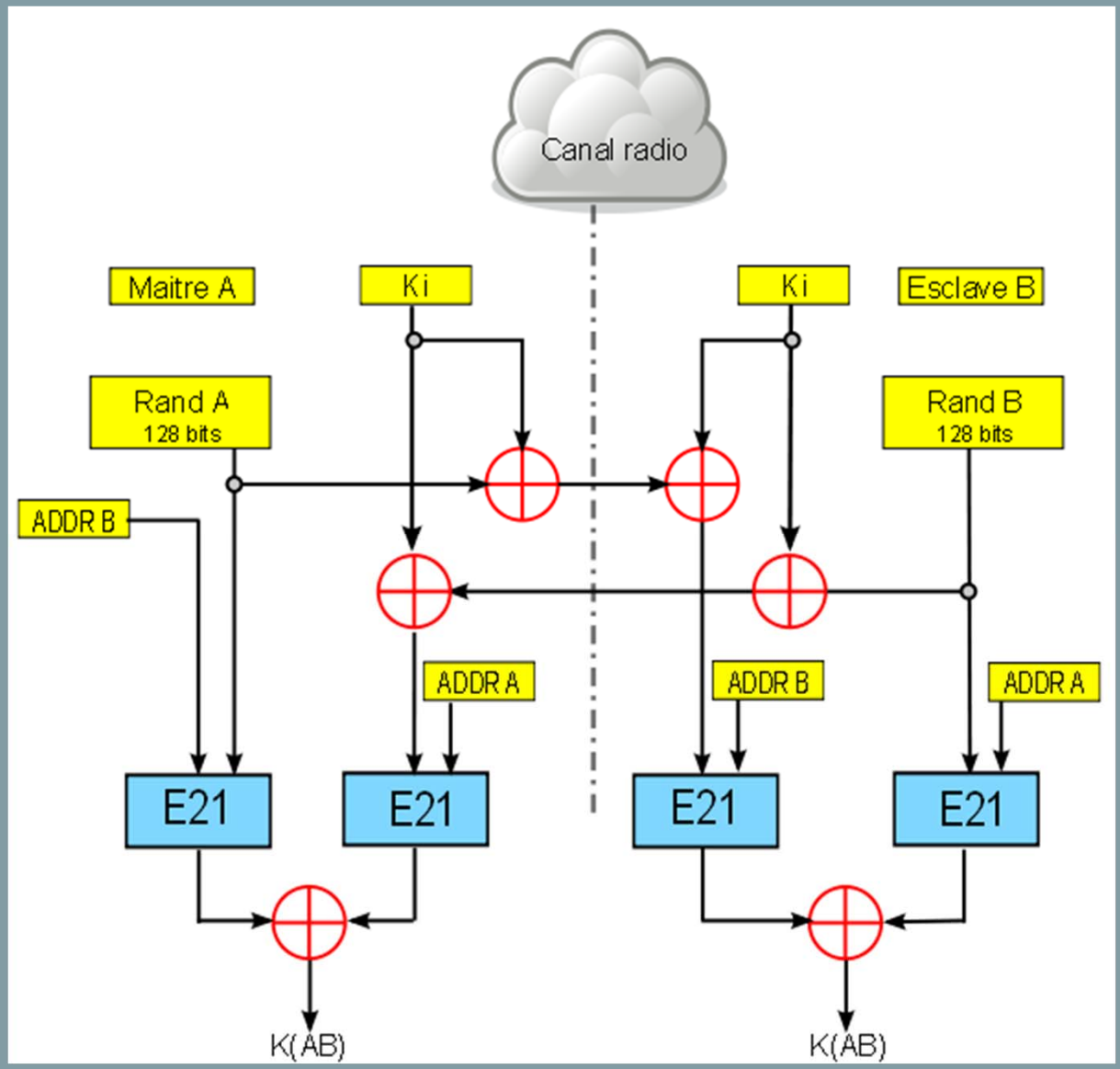
- Avant toute chose, le code PIN doit être tapé sur chaque appareil. Deux appareils ayant un code PIN fixe ne peuvent pas communiquer.
- La clef d'initialisation **Ki** est créée en utilisant l'algorithme **E22**. Elle est calculée à partir du code **PIN**, de l'adresse Bluetooth **ADDR** et d'un nombre aléatoire de 128 bits que nous noterons **RAND 0**.
- Cette clef est temporaire et va servir à engendrer une clef de chiffrement pour toute la session.

Clef d'initialisation. (2)



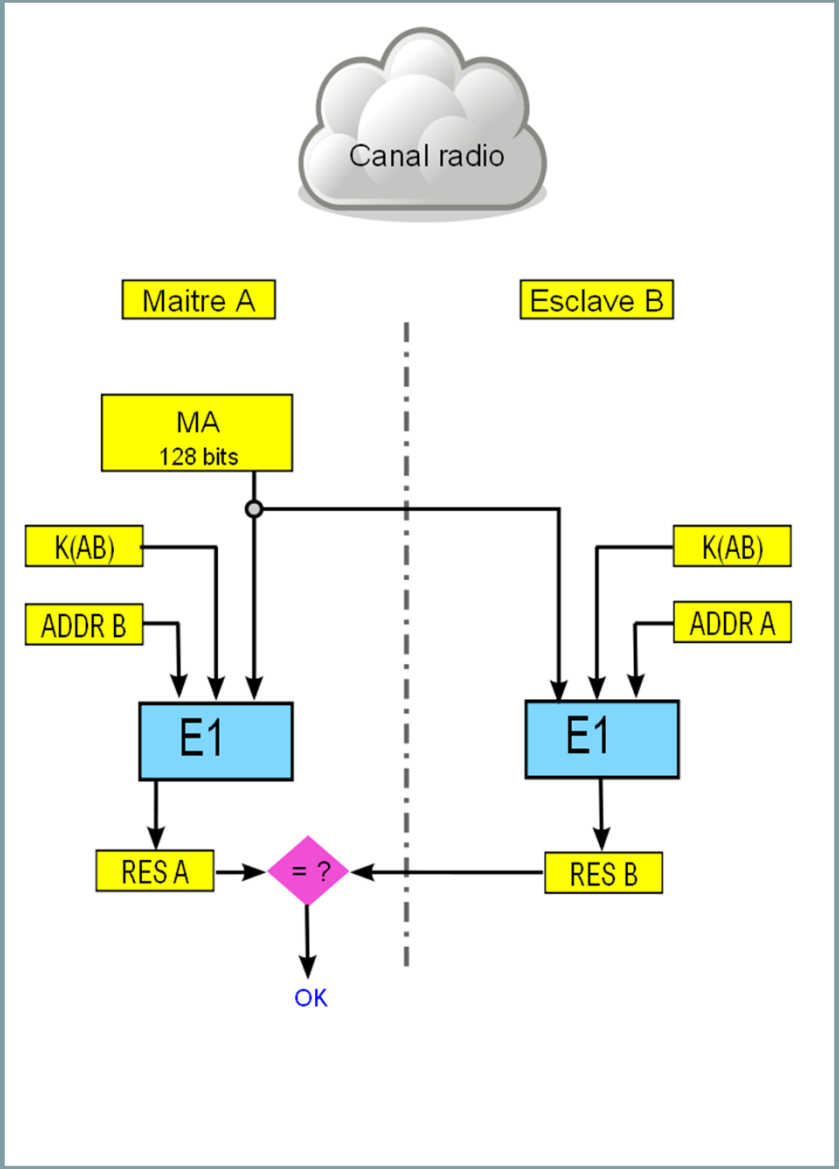
- La clef de chiffrement **K(AB)** se calcule comme suit :
  - A et B engendrent chacun un nombre aléatoire, noté respectivement **RAND A** et **RAND B**.
  - Ces nombres sont chiffrés avec **Ki** à l'aide d'un ou exclusif (méthode de Vernam) et sont échangés entre A et B.
  - A et B utilisent l'algorithme **E21** à deux reprises : une première fois pour calculer un nombre **LK A** à partir de **RAND A** et de **ADDR A** et une seconde fois à partir de **RAND B** et **ADDR B** pour calculer **LK B**.
  - Le ou exclusif de **LK A** et **LK B** est égal à la clef **K(AB)**.

Clef de chiffrement. (2)



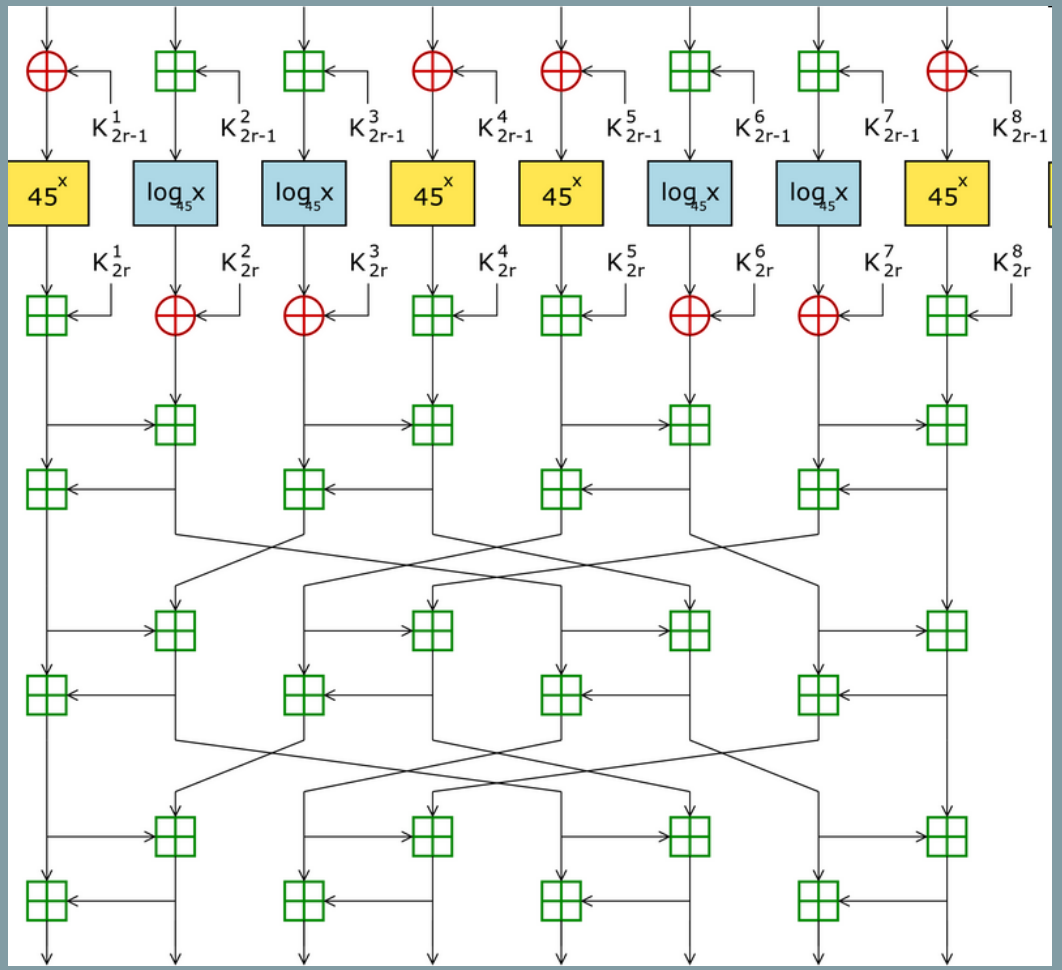
- La clef de chiffrement **K(AB)** étant créée, A envoie un nouveau nombre aléatoire de 128 bits noté **MA**.
- B calcule à partir de **K(AB)**, de son adresse **ADDR B** et de **MA** un nombre de 32 bits noté **RES B** qu'il renvoie à A. Ce nombre est calculé à partir de l'algorithme **E1**.
- A effectue le même calcul et obtient un nombre **RES A**.
- Si **RES A** et **RES B** sont égaux, l'authentification est un succès et la session peut débuter.

Authentification mutuelle. (2)



- Ils reposent tous les trois sur l'algorithme de chiffrement SAFER+ (présenté au même concours que l'AES).
- SAFER est un algorithme effectuant des rondes. Chaque ronde est divisée en quatre opérations :
  - Mélange avec une clef de session.
  - Brouillage par passage dans deux S-boites.
  - Second mélange avec une clef.
  - Diffusion par transformation de Hadamard.
- L'algorithme utilise également un processus de cadencement de la clef similaire à celui de l'AES.

Une ronde de l'algorithme SAFER.



- Il existe différents types d'attaques :
  - Attaque contre le code PIN durant la procédure de pairage.
  - Attaque algébrique contre l'algorithme E1.
  - Attaques sur les implémentations.

- La dernière attaque ne concerne pas un problème de cryptographie, mais différents problèmes de sécurité sur les appareils eux-mêmes. Nous n'en parlerons donc pas.

- Durant le pairage, les nombre aléatoires **RAND 0**, **MA**, **MB** et **RES B** passent en clair sur le canal et peuvent donc être capturés par une écoute radio.
- Un attaquant peut essayer tous les codes PIN possibles en exécutant l'algorithme E22. A chaque fois, il utilise la clef **Ki** produite et en déduit une valeur possible de **K(AB).**
- Il calcule alors **RES B** jusqu'à ce que la valeur corresponde à celle qui a transité sur le canal.
- A l'aide d'un PC de bureau, on peut en déduire le code PIN en moins d'une minute, si celui-ci a une taille inférieure à 7 chiffres.

- Il s'agit d'une attaque de type « force brute » qui teste toutes les clefs.
- On a montré qu'il suffisait de 2^{64} opérations pour obtenir une clef de 128 bits.
- La sécurité est donc équivalente à un algorithme à clef secrète de 64 bits.

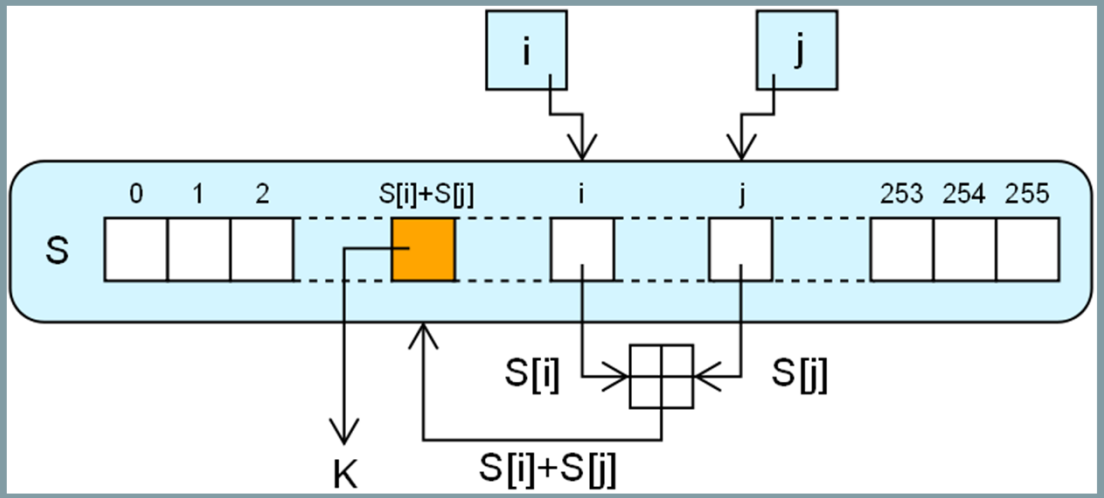
- Elle a beaucoup été discutée.
- On dispose de plusieurs algorithmes de chiffrement et d'authentification possibles.
- Certains ont déjà été cassés (WEP) d'autres sont fiables (WPA-AES).

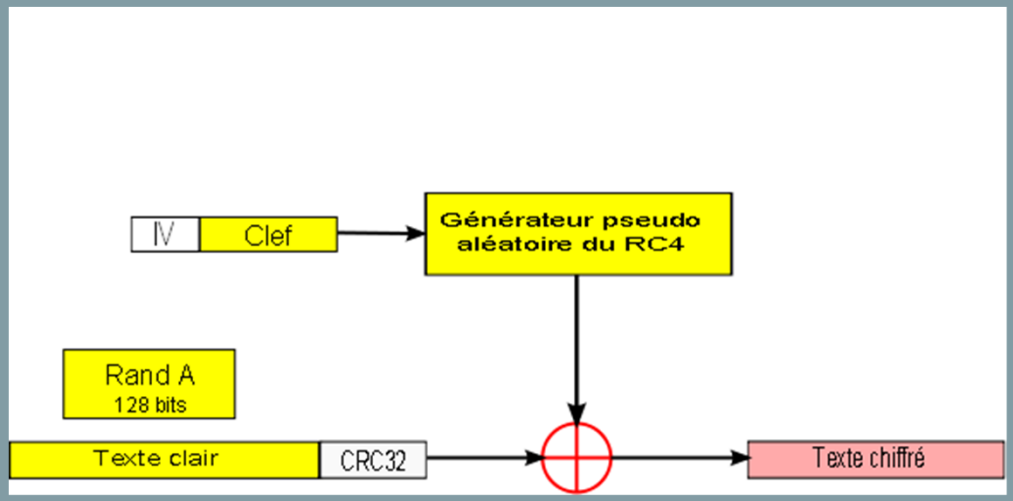
Le chiffrement par le WEP (Wired Equivalent Privacy). (1)

- C'est un protocole de chiffrement qui repose sur l'algorithme RC4 de Rivest.
- L'algorithme RC4 est un algorithme de chiffrement symétrique par flot, avec une clef secrète comprise entre 8 et 2048 bits.
- Dans le protocole, le réseau et les terminaux partagent une unique clef WEP.
- Cette clef est obtenue par concaténation d'une clef secrète de 40 ou 104 bits et d'un vecteur d'initialisation noté **IV** qui a une taille de 24 bits.

Le chiffrement par le WEP (Wired Equivalent Privacy). (2)

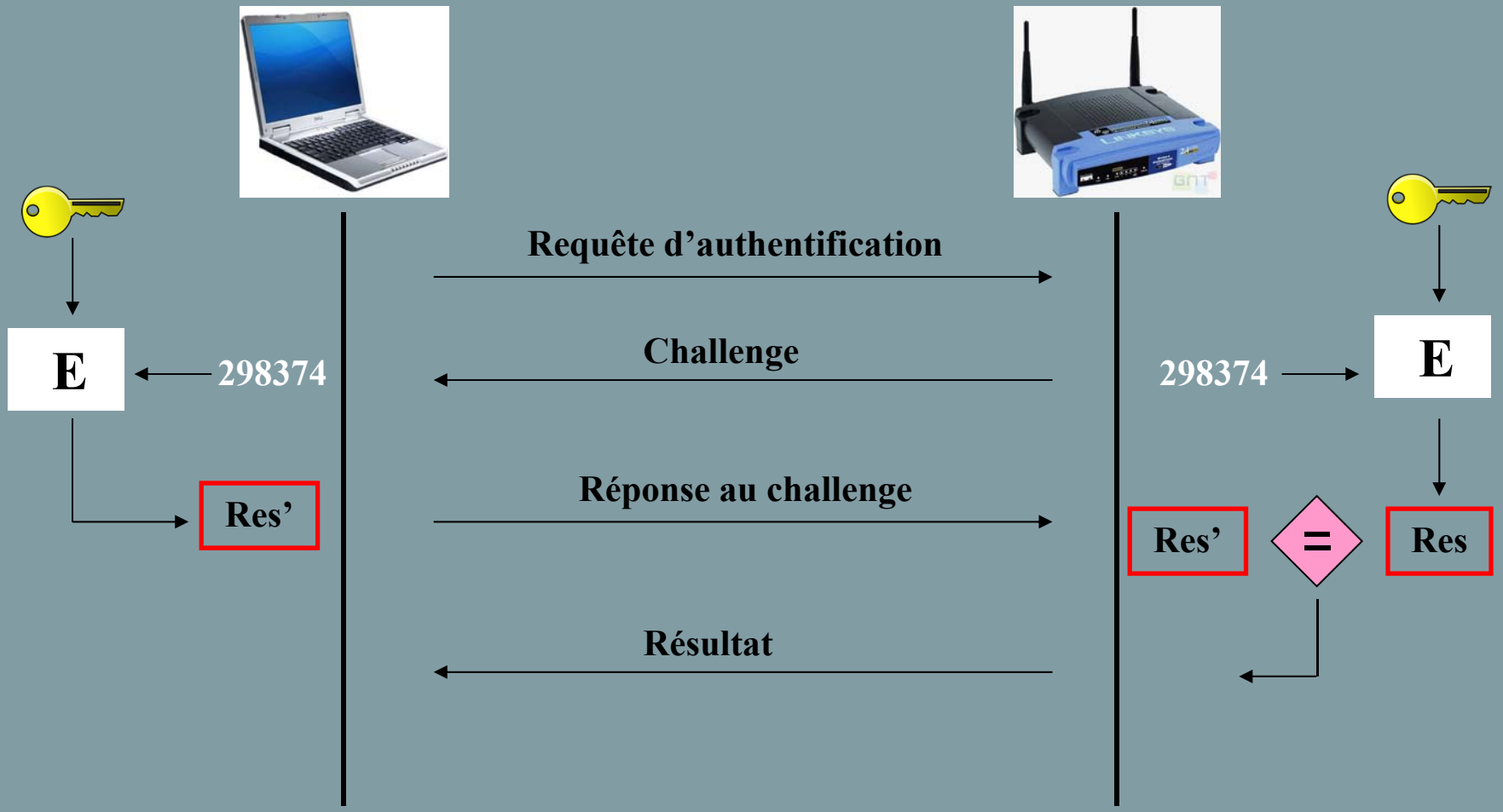
- Ce vecteur est modifié à chaque trame et la taille de la clef finale est de 64 ou 128 bits.
- Une fois la clef créée, le RC4 chiffre les données en continu (on parle de « stream cipher »).
- La clef est placée dans un générateur pseudo aléatoire qui détermine une séquence d'octets appelée keystream et que nous noterons **Ksi**.
- Ksi est ajouté à l'aide d'un ou exclusif au texte en clair, selon la méthode de Vernam.


i
j
0
1
2
S[i]+S[j]
i
j
253
254
255
S
S[i]
S[j]
K
S[i]+S[j]


IV
Clef
Générateur pseudo aléatoire du RC4
Rand A
128 bits
Texte clair
CRC32
Texte chiffré

- Il en existe deux :
  - Authentification ouverte.
  - Authentification à clef partagée.
- Le premier type n’offre aucune sécurité. Le second se déroule en quatre étapes :
  - Un appareil qui veut s’associer envoie une requête.
  - En réponse, le point d’accès envoie une trame contenant un « challenge » (nombre aléatoire qui va servir à un calcul commun).
  - La station chiffre le challenge avec sa clef secrète et l’envoie.
  - Le point d’accès déchiffre avec sa clef secrète et le compare avec le résultat de la station.

L’authentification par le WEP. (2)



- RC4 a été cryptanalysé par Shamir en 2001. Il suffit de quelques minutes pour récupérer la clef secrète.
- La clef de 40 bits est de toute façon trop courte.
- Il existe des attaques par collision permettant de casser la clef à partir de données récupérées en clair, en utilisant des collisions du vecteur **IV** :
  - La clef partagée ne change pratiquement jamais.
  - **IV** est concaténé à partir de cette clef. Comme ce vecteur ne fait que 24 bits, on peut effectuer une attaque par force brute.
  - Attaques sur les implémentations.

Des questions ?

Fin du chapitre 4. Crédits photos & copyright :

- Photo de couverture: © Adi Shamir.
- Dessin du puzzle: © Haykel Mejri.
- Photo nombres binaires: © Westwood Schools.
- Autres sources d'inspiration:
  - Cryptographie appliquée de Bruce Schneier, éditions Vuibert.
  - L'art du secret, in « dossier pour la science ».
  - Histoire des codes secrets, de Simon Singh, éditions livre de poche.