Criptografie și Securitate

- Prelegerea 7.2 -
WEP

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

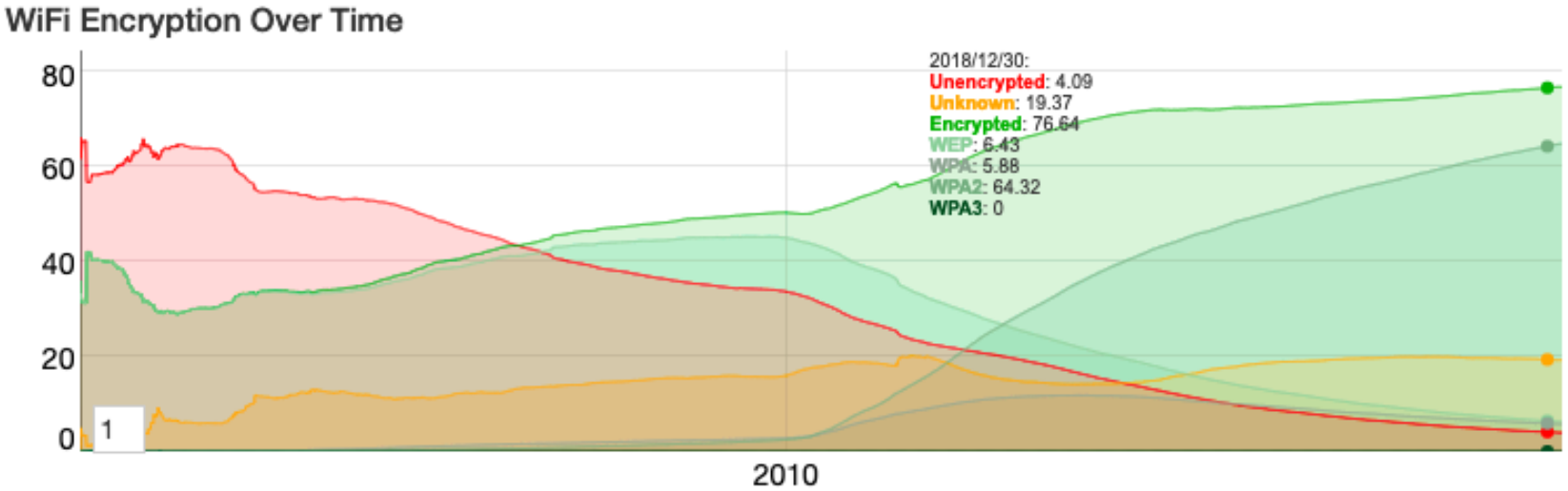
Cuprins

Informații generale

WEP este:

- definit ca standard IEEE 802.11 în 1999;
- folosit pentru criptare în cadrul rețelor fără fir;
- înlocuit de WPA, apoi WPA2.

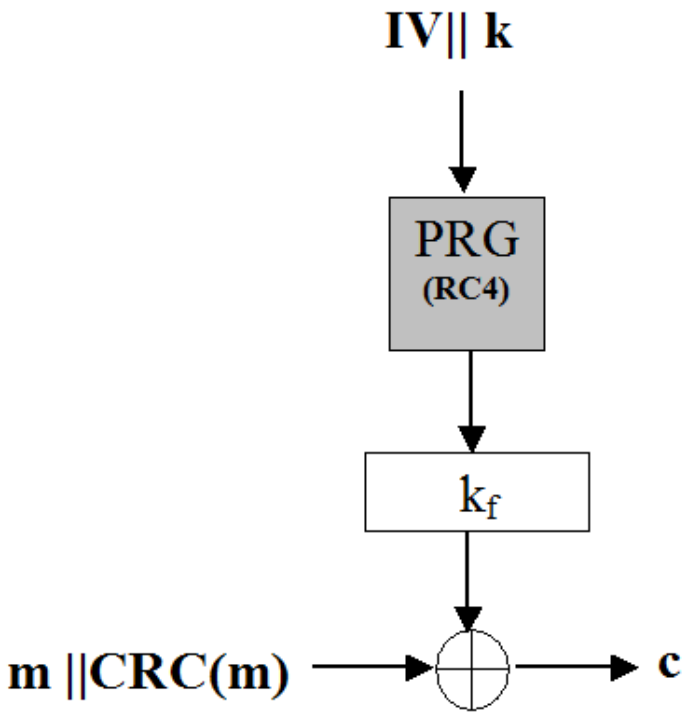
Informații generale



[https://wigle.net/stats]

Descriere

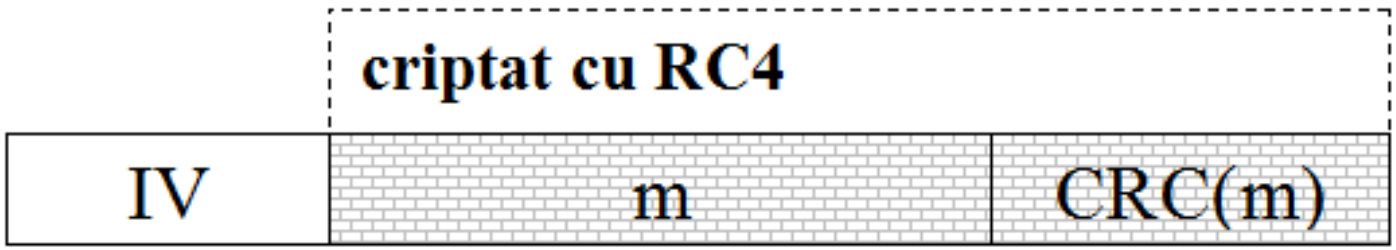
- WEP utilizează RC4;
- Introduce în plus (Cyclic Redundancy Check) cu rolul de a detecta eventuale erori de transmisiune;
- IV este transmis către destinatar, împreună cu c ($IV||c$), fiind necesar pentru decriptare .



Descriere

Detalii de implementare:

- $|IV| = 24$ (biți)
- IV se utilizează în *counter mode* (0, 1, 2, . . .)



Securitate - Problema 1

Problema 1: Utilizarea multiplă a lui IV

- Întrebare: Ce efect imediat are utilizarea multiplă a lui IV pentru o cheie fixată k?

Securitate - Problema 1

Problema 1: Utilizarea multiplă a lui IV

- Întrebare: Ce efect imediat are utilizarea multiplă a lui IV pentru o cheie fixată k?
- Răspuns: Se obține întotdeauna aceeași cheie fluidă k_r

$$IV_1 = IV_2 = IV \Rightarrow k_{f1} = k_{f2} = PRG(IV||k)$$

Securitate - Problema 1

Problema 1: Utilizarea multiplă a lui IV

- Întrebare: Ce efect imediat are utilizarea multiplă a lui IV pentru o cheie fixată k?
- Răspuns: Se obține întotdeauna aceeași cheie fluidă k_r

$$IV_1 = IV_2 = IV \Rightarrow k_{f1} = k_{f2} = PRG(IV||k)$$

- Întrebare: Sistemul rămâne sigur în aceste condiții?

Securitate - Problema 1

Problema 1: Utilizarea multiplă a lui IV

- Întrebare: Ce efect imediat are utilizarea multiplă a lui IV pentru o cheie fixată k?
- Răspuns: Se obține întotdeauna aceeași cheie fluidă k_r

$$IV_1 = IV_2 = IV \Rightarrow k_{f1} = k_{f2} = PRG(IV||k)$$

- Întrebare: Sistemul rămâne sigur în aceste condiții?
- Răspuns: NU!

$$c_1 = m_1 \oplus k_{f1}, c_2 = m_2 \oplus k_{f2} \Rightarrow c_1 \oplus c_2 = m_1 \oplus m_2$$

Exemplu:

- dacă $\mathcal{A}$ cunoaște m_1, atunci poate determina m_2
- $\mathcal{A}$ poate determina m_1 și m_2 folosind analiza statistică

Securitate - Problema 1

- Întrebare: Câte valori posibile poate lua IV?

Securitate - Problema 1

- Întrebare: Câte valori posibile poate lua IV?
- Răspuns: 2^{24}

Securitate - Problema 1

- Întrebare: Câte valori posibile poate lua IV?
- Răspuns: 2^{24}
- Cum un AP (Access Point) trimite aproximativ 1000 pachete/s, valoarea lui IV se repetă la cel mult la câteva ore!

Securitate - Problema 1

- Întrebare: Câte valori posibile poate lua IV?
- Răspuns: 2^{24}
- Cum un AP (Access Point) trimite aproximativ 1000 pachete/s, valoarea lui *IV* se repetă la cel mult la câteva ore!
- Mai mult, există echipamente care resetează *IV* la fiecare repornire!

Securitate - Problema 2

Problema 2: Liniaritatea

- Întrebare: Făcând abstracție de CRC, $\mathcal{A}$ poate modifica mesajul criptat transmis după bunul său plac?

Securitate - Problema 2

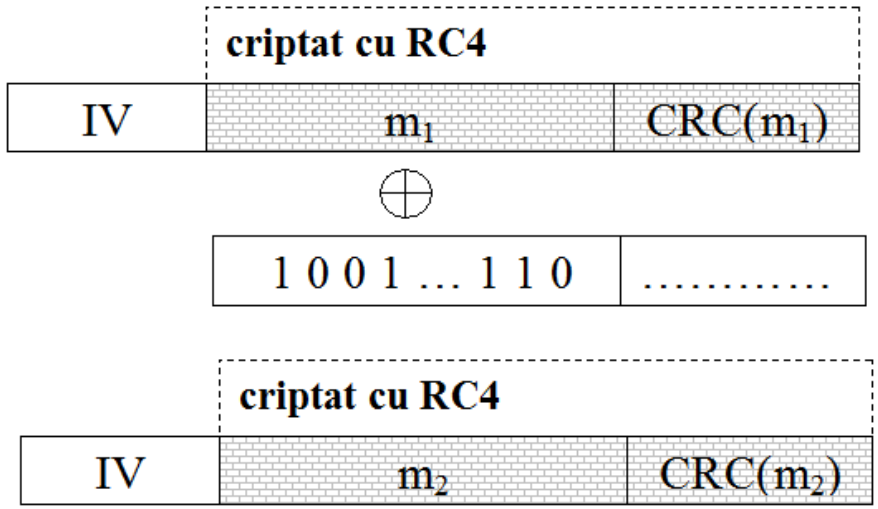
Problema 2: Liniaritatea

- Întrebare: Făcând abstracție de CRC, $\mathcal{A}$ poate modifica mesajul criptat transmis după bunul său plac?
- Răspuns: DA!

$$(m_1 \oplus m_2) \oplus k_f = (m_1 \oplus k_f) \oplus m_2$$

Exemplu:

- $\mathcal{A}$ interceptează c_1 și îl transformă în c_2



Securitate - Problema 2

- CRC poate detecta erorile de transmisiune (neintenționate) dar nu și modificarile premeditate (intenționate)

Securitate - Problema 2

- CRC poate detecta erorile de transmisiune (neintenționate) dar nu și modificarile premeditate (intenționate)
- În aceste condiții, $\mathcal{A}$ poate modifica mesajele transmise:
  - prin XOR-are cu secvențe (convenabile) de biți
  - prin amestecarea biților din mesajul interceptat

Important de reținut!

- O proastă implementare / utilizare poate diminua considerabil securitatea unui sistem!