Stream Ciphers

Cryptography and Protocols
Andrei Bulatov

Pseudorandom Generators

- Let T(n), ε(n) be functions. A collection $\{X_n\}$ of random variables with $X_n \in \{0,1\}^n$ is called (T,ε)-pseudorandom if $\{X_n\} \approx_{T,\varepsilon} \{U_n\}$
- A collection of functions $g_n : \{0,1\}^n \to \{0,1\}^{m(n)}$ is called a (T,ε)-pseudorandom generator if $\{g_n(U_n)\}$ is (T,ε)-pseudorandom
- m(n) – n > 0 the stretch of a PRG
- A PRG should be (T,ε)-pseudorandom for some superpolynomial pair (T,ε)
- g_n must be efficiently computable
- RC4 and Blum-Blum-Shub

Stream Ciphers

- Let $\{g_n\}$ be a pseudorandom generator producing, given a seed of length n, bit strings of length m(n)

- Let (K,E,D) be a SES defined as follows:

  K – draws keys uniformly at random

  E – to encrypt a plaintext P of length m(n) it applies g_n to the key k and computes

$$C_i = (g_n(k))_i \oplus P_i$$

  D – same as E

Security of Stream Ciphers

- **Theorem**.

  Let $\{g_n\}$ be a (T,ε)- pseudorandom generator. Then the SES constructed as above is (T,2ε)-secure.

- **Proof**.

  Indistinguishability:

  Let T(n) and ε(n) be functions on natural numbers. Collections of random variables $\{X_n\}$ and $\{Y_n\}$ such that $X_n, Y_n \in \{0,1\}^n$ are said to be computationally (T,ε)-indistinguishable , if for any probabilistic algorithm Alg with time complexity at most T(n)

  $$|\Pr[\mathrm{Alg}(X_n)=1]-\Pr[\mathrm{Alg}(Y_n)=1]| \le \varepsilon(n)$$

  Pseudorandomness:

  Let T(n), ε(n) be functions. A collection $\{X_n\}$ of random variables with $X_n \in \{0,1\}^n$ is called (T,ε)-pseudorandom if $\{X_n\} \approx_{T,\varepsilon} \{U_n\}$

  Security:

  (K,E,D) is computationally secure if for any $P_1, P_2 \in \{0,1\}^{m(n)}$ distributions $E_{U_n}(P_1)$ and $E_{U_n}(P_2)$ are (T,ε)-indistinguishable

Security of Stream Ciphers (cntd)

- Suppose that (K,E,D) is not secure

  There is algorithm Eve of time complexity at most T, and P_1, P_2 (actually sequences $\{P_1^n\},\{P_2^n\}$ with $P_1^n, P_2^n \in \{0,1\}^{m(n)}$) such that

$$|\Pr[\text{Eve}(E_{U_n}(P_1^n)) = 1] - \Pr[\text{Eve}(E_{U_n}(P_2^n)) = 1]| \ge 2\varepsilon(n)$$

- We have

$$|\Pr[\text{Eve}(g_n(U_n) \oplus P_1^n) = 1] - \Pr[\text{Eve}(U_{m(n)}) = 1]| +$$
$$|\Pr[\text{Eve}(U_{m(n)}) = 1] - \Pr[\text{Eve}(g_n(U_n) \oplus P_1^n) = 1]| \ge$$

$$|\Pr[\text{Eve}(g_n(U_n) \oplus P_1^n) = 1] - \Pr[\text{Eve}(g_n(U_n) \oplus P_2^n) = 1]| \ge 2\varepsilon(n)$$

- Therefore , say,

$$|\Pr[\text{Eve}(g_n(U_n) \oplus P_1^n) = 1] - \Pr[\text{Eve}(U_{m(n)}) = 1]| \ge \varepsilon$$

Security of Stream Ciphers (cntd)

- Observe that $U_{m(n)} \oplus P_1^n = U_{m(n)}$
- Let Eve'(C) = Eve(C $\oplus P_1^n$). Clearly, its complexity is at most T
- Then

$$|\Pr[\text{Eve}(g_n(U_n) \oplus P_1^n) = 1] - \Pr[\text{Eve}(U_{m(n)}) = 1]|$$

$$= |\Pr[\text{Eve}(g_n(U_n) \oplus P_1^n) = 1] - \Pr[\text{Eve}(U_{m(n)} \oplus P_1^n) = 1]|$$

$$= |\Pr[\text{Eve'}(g_n(U_n)) = 1] - \Pr[\text{Eve'}(U_{m(n)}) = 1]| \geq \varepsilon(n)$$

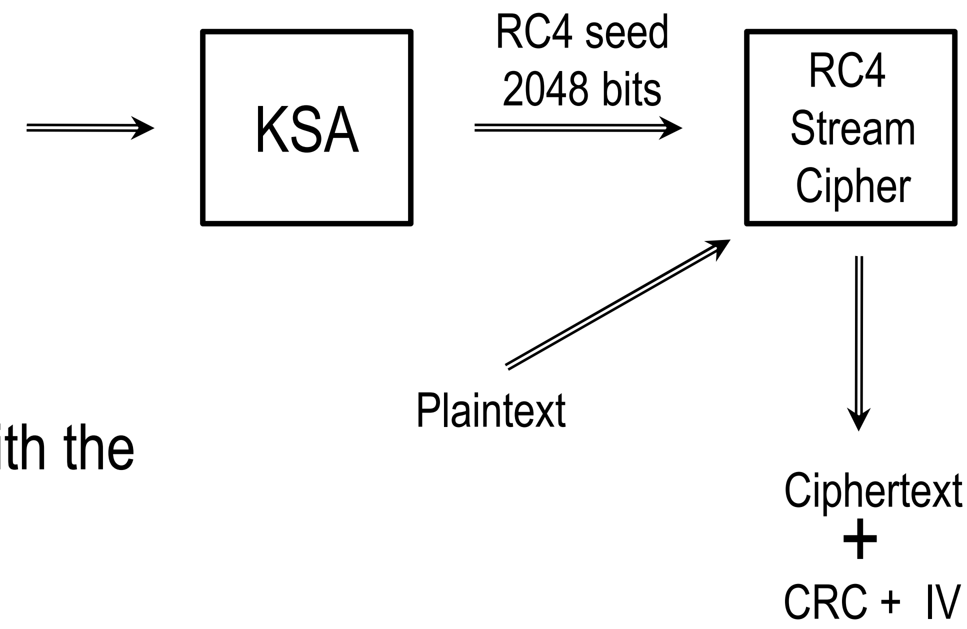
- A contradiction.

WEP – Wired Equivalent Privacy

- WEP ≈ handshaking +
  encryption +
  authentication

- Encryption

WEP Key
104 bits = 26 hexadec. + Initialization Vector (IV) 24 bits



- IV is just a counter
- WEP Key is associated with the network and fixed

Key Scheduling Algorithm

- KSE, the Key Scheduling Algorithm – that uses an input of length $40 \leq n \leq 128$ to generate S
- Input: a key k of length n, $40 \leq n \leq 128$

  for i **from** 0 **to** 255 S[i] := i **endfor**

  j := 0

  for i **from** 0 **to** 255

  j := (j + S[i] + k[i mod n]) mod 256

  swap(S[i],S[j])

  endfor

Handshaking

- Shared Key Handshaking 4 steps

  The client station sends an authentication request to the Access Point.

  The Access Point sends back a clear-text challenge.

  The client has to encrypt the challenge text using the configured WEP key, and send it back in another authentication request.

  The Access Point decrypts the material, and compares it with the clear-text it had sent. Depending on the success of this comparison, the Access Point sends back a positive or negative response.

Attacks

- There dependencies between the seed and initial bytes
- KSA is the weakest link
- Known IV + KSA weaknesses = the Key can be recovered after intercepting as few as 40000 packets
- Later improvement: the key can be recovered after 15-20 min of listening of a fully loaded network

Fixes

- WPA2 (Wi-Fi Protected Access) uses block cipher AES instead of RC4. Not frequently used these days, as it requires upgrades of hardware of access points
- WPA. Interim protocol between WEP and WPA2
- Encryption in WPA