Generarea, derivarea, schimbul si managementul cheilor criptografice

Autor: Alina-Elena BRINZA
Indrumator de licenta: Ferucio Laurentiu Tiplea

Iulie 2017

Cuprins

- Necesitate in contextul protocolului SSL/TLS
- Generarea cheilor criptografice
- Derivarea cheilor criptografice
- PUF - Phisically Unclonable Functions

Necesitate in contextul protocolului SSL/TLS

- Argumentare
- Initiere in termeni criptigrafici si de securitate
  - (sistem de criptare, securitate, criptografie simetrica, criptografie asimetrica, bit security, securitate IND-CPA, functii hash, "numar random")
- Evolutia securitatii in timp
- SSL/TLS - scurta prezentare a protocolului
  - (autentificare, confidentialitate, handshake)

Generarea cheilor criptografice

- Generarea cheilor simetrice si asimetrice
- Generatori si functii pseudo-random
- RC4 & NOMORE attack

Derivarea cheilor criptografice

- Descriere generala KDF (Key Derivation Functions)
- PBKDF & HKDF
  - (generare si verificare MAC)
- Concat KDFHash & KDFHMAC
- Moduri KDF
  - (Counter Mode, Feedback Mode, Double Pipeline Iteration Mode)

PUF - Phisically Unclonable Functions

- Tipuri principale de PUF
  - PUF-uri optice, decalate,SRAM, fluture
- Aplicatii ale PUF-urilor
  - Abordari anti-frauda

Contributii

Algoritmul lui Pollard:

Calcularea lui γ astfel incat pow(α,γ) = β, β ϵ grupului ciclic G generat de α.

Algoritmul lui Pollard
G grup ciclic de ordin p, α, β ϵ $G = S0, S1, S2$. (G=$S0$ U $S1$ U $S2$)

Input: a, generator al grupului G, b element ϵ din G.
Output:x astfel incat a^x=b sau esec.

Contributii

Algoritmul lui Pohlig-Hellman

Calcularea logaritmului discret intr-un grup comutativ a carui ordin este un numar intreg a carui factorizare se face pe baza unor numere prime mici.

Contributii

Algoritmul lui Pohlig-Hellman

Input: G un grup ciclic de ordin n, g generator ϵ G, h ϵ G, n factorizarea prima.
Output: x ϵ 0,1,..,n-1 astfel incat g^x=h, x fiind unic.

Cum functioneaza?

Pentru a putea ataca schimbul de chei Diffie-Hellman, un atacator ar putea extrage cheia secreta de la o cheie publica p$k1$=g^a (mod p) si apoi calcula cheia partajata g^{ab} (mod p) folosind cheia publica p$k2 = g^b$ (mod p).

O abordare relativ rapida, de complexitate $\sqrt{q}$ pentru gasirea solutiei, o reprezinta algoritmul Pohlig-Hellman.

Cum functioneaza?

Cunoscand factorizarea completa a ordinului grupului, factorii fiind relativ mici, logaritmul discret poate fi calculat cu usurinta. Ideea principala este gasirea valorii secrete modulo divizorii ordinului grupului, reducand cheia publica in subgrupuri de ordine ce divid ordinul grupului.

Prin TCR, cheia secreta poate fi reasamblata in oridnul grupului iar calcularea cheii secrete se face modulo fiecare factor *pi* la puterea *ki* al ordinului.

Cum functioneaza?

O modalitate de a face aceste calcule este reducerea cheii secrete la subgrup. Calculand logaritmul discret al valorii y la puterea (ϕp / (*pi* la puterea *ki*)), obtinem cheia secreta (mod (*pi* la puterea *ki*)).

Valoarea obtinuta este un generator al subgrupului de ordin *pi* la puterea *ki* ridicat la puterea cheiaSecreta1. Continuand si aplicand teorema chineza a resturilor, obtinem cheia secreta finala.

Concluzie

- "Whoever is careless with the truth in small matters cannot be trusted with important matters" (Albert Einstein)
- "We cannot solve our problems with the same thinking we used when we created them" (Albert Einstein)
- Insanity: doing the same thing over and over and expecting different results" (Albert Einstein)
- "I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones" (Albert Einstein)