Generarea, derivarea, schimbul și managementul cheilor criptografice

Autor: Alina-Elena BRINZA
Îndrumător de licență: Ferucio Laurențiu Țiplea

Iulie 2017

Cuprins

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

Necesitate în contextul protocolului SSL/TLS

- Argumentare
- Inițiere în termeni criptografici și de securitate
  - (sistem de criptare, securitate, criptografie simetrică, criptografie asimetrică, securitate semantică, securitate IND-CPA, funcții hash, "număr random")
- Evoluția securității în timp
- SSL/TLS - scurtă prezentare a protocolului
  - (autentificare, confidențialitate, handshake)

Generarea cheilor criptografice

- Generarea cheilor simetrice și asimetrice
- Generatori și funcții pseudo-random
- RC4 & NOMORE attack

Derivarea cheilor criptografice

- Descriere generala KDF (Key Derivation Functions)
- PBKDF & HKDF
  - (generare și 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
- Aplicații ale PUF-urilor
  - Abordări anti-fraudă

Contribuții

Algoritmul lui Pollard:

Calcularea lui γ astfel încât 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 încât a^x=b sau eșec.

Contribuții

Algoritmul lui Pohlig-Hellman

Calcularea logaritmului discret într-un grup comutativ a cărui ordin este un număr întreg a cărui factorizare se face pe baza unor numere prime mici.

Contribuții

Algoritmul lui Pohlig-Hellman

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

Cum funcționează?

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

O abordare relativ rapidă, de complexitate $\sqrt{q}$ pentru găsirea soluției, o reprezintă algoritmul Pohlig-Hellman.

Cum funționează?

Cunoscând factorizarea completă a ordinului grupului, factorii fiind relativ mici, logaritmul discret poate fi calculat cu ușurință. Ideea principală este găsirea valorii secrete modulo divizorii ordinului grupului, reducând cheia publică în subgrupuri de ordine ce divid ordinul grupului.

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

Cum funcționează?

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

Valoarea obținută este un generator al subgrupului de ordin *pi* la puterea *ki* ridicat la puterea cheiaSecretă1. Continuând și aplicând teorema chineza a resturilor, obținem cheia secretă finală.

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)