

ATTACK ALGORITMA CRAMER-SHOUP BERBASIS LOGARITMA DISKRIT

www.noersilo.webid | noersilo@yahoo.com

A. Algoritma Cramer-Shoup

The Cramer-Shoup public key cryptosystem aman terhadap chosen ciphertext attacks. Hal ini didasarkan pada Decision Diffie-Hellman problem dan keberadaan dari collision fungsi hash. Skema algoritma ini hanya melibatkan beberapa eksponensiasi atas grup, sehingga skema lebih efisien dari segi komputasi.

Cramer-Shoup menggunakan grup G dari order prima q dimana nilai q besar. Cramer juga menggunakan collision fungsi hash H yang meng-hash string yang panjang yang nilainya terkandung dalam Z_q . Kunci private di Cramer-Shoup ada enam nilai $(x_1, x_2, y_1, y_2, z_1, z_2)$, yang semuanya dipilih secara acak dari Z_q . Kunci publiknya termasuk nilai-nilai dari g_1 dan g_2 yang dipilih secara acak dari G . Kunci publiknya juga mencakup tiga nilai sebagai berikut :

$$c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}, h = g_1^{z_1} g_2^{z_2} \quad (C.26)$$

Sehingga kunci publiknya adalah (g_1, g_2, c, d, h) .

Setelah cipherteks sudah diterima, langkah pertama yang dilakukan receiver setelah menerima cipherteks adalah melakukan verifikasi terhadap integritasnya. Hal ini dilakukan dengan menghitung $\alpha = H(u_1, u_2, e)$ lalu memverifikasi seperti persamaan berikut :

$$v \stackrel{?}{=} u_1^{x_1} u_2^{x_2} (u_1^{y_1} u_2^{y_2})^\alpha \quad (C.28)$$

Jika tidak memenuhi, maka pesan tersebut akan di *reject*. Jika persamaan tersebut terpenuhi, maka dilakukan pada proses dekripsinya, yaitu :

Pembuktian :

$$u_1^{x_1} u_2^{x_2} = g_1^{rx_1} g_2^{rx_2} = c^r$$

Karena $u_1 =$ dan $u_2 =$ maka :

Karena $u_1^{-z_1} u_2^{-z_2} = g_1^{-rz_1} g_2^{-rz_2} = h^{-r}$, maka :

$$e u_1^{-z_1} u_2^{-z_2} = h^r m h^{-r} = m$$

B. Setup Attack on Cramer-Shoup Algorithm

Kunci public pada algoritma Cramer-Shoup adalah (g_1, g_2, c, d, h) dan ciphertext-nya adalah (u_1, u_2, e, v) . Diasumsikan G adalah subgroup siklik dari Z_p^* , dimana p adalah bilangan prima. Diberikan 2 langkah enkripsi dalam Cramer-Shoup yakni (u_1, u_2, e, v) merupakan enkripsi dari m yang menggunakan r sebagai nonce dan (u_1', u_2', e', v') yang menggunakan r' sebagai nonce.

Langkah awal untuk mengidentifikasi kleptogram yaitu :

- U_1 adalah modular exponensiasi
- Ketika ciphertext dikirim melalui jaringan public, nilai u_1 dapat diambil oleh penyerang
- Exponen r digenerate dengan algoritma enkripsi Cramer-Shoup sehingga available untuk algoritma enkripsinya
- Misal r sebagai 'fed' dari inputan `GenPrivateExponen2`
- Hitung $r' = \text{GenPrivateExponen}(r)$ instead of pemilihan r' yang random. Outputnya merupakan random nonce yang akan digunakan dalam enkripsi kedua

Penyerang dapat memperoleh $u_1 = g^r \text{ mod } p$ dari komunikasi publik. Dengan menghitung $u_1^x \text{ mod } p$ dan menambah O seperlunya, nilai T_0 dapat diperoleh oleh penyerang. Hasilnya, penyerang dapat menghitung $r' = F_1(T_0 || \text{ID} || i)$ dengan menebak ID dan i . Dalam serangan pada Diffie-Hellman, semua serangan dapat ditebak kebenarannya. Ketika r' dapat menghitung r' , penyerang dapat menghitung pesan $m' = e' h^{-r'} \text{ mod } p$. Serangan ini dapat dihentikan dengan cara yang sama seperti serangan pada Diffie-Hellman key exchange.