Dokumentasi Protokol

# Login

Login dilakukan dengan menggunakan mekanisme pengamanan dengan pertukaran kunci ***Diffie-Hellman Key Exchange Algorrithm*** terlebih dahulu lalu *username* dan *password* dikirimkan terenkripsi dengan algoritma ***Advanced Encryption Standard* (AES)** dengan kunci hasil pertukaran yang dilakukan sebelumnya.

Urutan:

1. Client mengirimkan pesan berisi kode MSG\_LOGIN.

|  |
| --- |
| MSG\_LOGIN (byte) |

1. Server membalas dengan pesan berisi nilai ***p*** dan ***g*** dalam format UTF.

|  |  |
| --- | --- |
| p (UTF) | g (UTF) |

1. Client lalu membuat pasangan kunci publik dan private. Panjang kunci publik dalam satuan byte (CLI\_PUB\_LENGTH) dan isi dari kunci publik (CLIPUB) ini lalu dikirimkan ke server.

|  |  |
| --- | --- |
| CLI\_PUB\_LENGTH (int) | CLI\_PUB (bytes) |

1. Server lalu membalas dengan panjang kunci publik dalam satuan byte (SERV\_PUB\_LENGTH) dan isi dari kunci publik milik server (SERV\_PUB) ke Client.

|  |  |
| --- | --- |
| SERV\_PUB\_LENGTH (int) | SERV\_PUB (bytes) |

1. Client kemudian akan menghasilkan *secret code* bersama. Lalu username dan password akan dienkripsi dengan AES menjadi AES\_UNAME dan AES\_PASSWD. Client akan mengirimkan secara berturut-turut panjang dari AES\_NAME (AES\_UNAME\_LENGHTH), AES\_UNAME, panjang dari AES\_PASSWD (AES\_PASSWD\_LENGTH), dan AES\_PASSWD ke server.

|  |  |  |  |
| --- | --- | --- | --- |
| AES\_UNAME\_LENGHTH (int) | AES\_UNAME (bytes) | AES\_PASSWD\_LENGTH (int) | AES\_PASSWD (bytes) |

1. Server akan mendekripsi *username* dan *password* yang dikirimkan tadi dengan terlebih dahulu menghasilkan *sercet code* bersama.
   1. Jika data login benar, maka akan dikirimkan pesan berisi kode MSG\_SUCCESS.

|  |
| --- |
| MSG\_SUCCESS (byte) |

* 1. Jika data login salah, maka akan dikirimkan pesan berisi kode MSG\_FAILED.

|  |
| --- |
| MSG\_FAILED (byte) |