

PENERAPAN ALGORITMA *BLOWFISH* DAN *ELGAMAL* UNTUK PENGAMANAN DATA SEKUNDER *DATABASE*

Harry Darmawan Siregar

ABSTRAK

Perkembangan teknologi mengakibatkan pemanfaatan teknologi informasi salah satunya pemanfaatan pada *E-commerce*. *E-commerce* diterapkan pada berbagai *platform* seperti *personal computer*(PC) dan *mobile smartphone*. Karena banyak berbagai *platform* maka banyak juga penggunaanya. Para pengguna *E-commerce* melakukan *register* yang mengharuskan memasukan nomor telepon, nama dan alamat dimana data-data tersebut adalah data sekunder yang tidak dilindungi keamanan pada *database*. Data tersebut sangatlah penting karena dapat disalahgunakan oleh pihak tidak bertanggung jawab seperti menjual data tersebut. Berdasarkan dari kasus tersebut penelitian ini ingin meneliti untuk meningkatkan keamanan informasi data sekunder dengan penerapan kombinasi algoritma *Blowfish* dan *Elgamal* pada data sekunder *database* agar dapat dilindungi jika terjadi kebocoran data. Pengamanan data dengan melakukan enkripsi dengan *Blowfish* kemudian cipherteks akan kembali dienkripsi lagi dengan *Elgamal* diharapkan dapat meningkatkan keamanan data pada *database* sehingga pengguna *E-commerce* dapat merasa lebih aman saat mempercayakan datanya saat registrasi. Hasil luaran yang didapatkan dari penelitian ini adalah penerapan algoritma *Blowfish* dan algoritma *Elgamal* dapat meningkatkan keamanan data dari serangan *brute force attack* pada cipherteks data sekunder pada *database* dengan penerapan pada perangkat lunak berbasis *website* dengan waktu proses enkripsi dan dekripsi serta penggunaan sumber daya yang cukup efisien.

Kata Kunci : *database*, *Blowfish*, *Elgamal*, data sekunder.

APPLICATION OF BLOWFISH AND ELGAMAL ALGORITHM FOR DATABASE SECONDARY DATA SECURITY

Harry Darmawan Siregar

ABSTRACT

Technological developments have resulted in the use of information technology, one of which is the usage of e-commerce. E-commerce had been applied to various platforms such as personal computers (PCs) and mobile smartphones. Because there are many different platforms, there are also many *users*. The *users* of E-commerce are required to insert their personal data such as phone number, name, and address where those data are called secondary data in a database which is not secured almost on all databases. This kind of data are can be very important too because the irresponsible people who steal and got this data can abuse it to do bad things like selling it. Based on this case, this research wants to research how to improve the security of secondary data information by applying the combination of Blowfish and Elgamal algorithms to the secondary data database so that it can be more secured in case if there is data leakage. Data security by encrypting with Blowfish then ciphertext will be re-encrypted again with Elgamal is expected to improve data security in the database so that E-commerce *users* can feel more secure when entrusting their data during registration. The output obtained from this research are the application of the Blowfish algorithm and the Elgamal algorithm which can improve data security from possibility of brute force attacks on secondary data ciphertext in the database by applying it to website-based software with encryption and decryption process time and efficient use of resources.

Keywords : *database, Blowfish, Elgamal, secondary data.*