Jurnal Sistim Informasi dan Teknologi
https://jsisfotek.org/index.php
2019 Vol. 1 No.4 Hal: 66-72 e-ISSN: 2686-3154

Kerahasiaan Teks Basis Data MySQL Menggunakan Algoritma Elgamal

Niko Surya Atmaja[1]✉, Yuhandri Yunus[2], Sumijan[3]
[1,2,3]Fakultas Ilmu Komputer, Univeritas Putera Indonesia YPTK Padang
niko.suryaatmaja@gmail.com

Abstract

The common method used to secure a MySQL database is in access control. The technique is the use of a password. To better secure the data sent cryptographic techniques need to be done. This study uses the Elgamal method in conducting cryptography. The results of this study generate MySQL databases in random form during safer delivery and can only be accessed by parties who have a password. So this research can further improve MySQL data security.

Keywords: Confidentiality, Cryptography, Elgamal algorithm, Database, MySQL.

Abstrak

Cara yang umum digunakan untuk mengamankan basis data MySQL adalah dalam pengendalian akses. Tekniknya adalah penggunaan kata sandi. Untuk lebih mengamankan data yang dikirim perlu dilakukan teknik kriptografi. Penelitian ini menggunakan metode elgamal dalam melakukan kriptografi. Hasil dari penelitian ini menghasilkan basis data MySQL dalam bentuk acak selama pengiriman lebih aman dan hanya dapat diakses oleh pihak yang mempunyai sandi. Sehingga penelitian ini dapat lebih meningkatkan keamanan data MySQL.

Kata kunci: Kerahasiaan, Kriptografi, Algoritma Elgamal, Basis data, MySQL.

1. Pendahuluan

Pencuri data adalah orang yang tidak berhak mengakses sebuah basis data. Orang ini berada di dalam atau di luar sistem. Para pecuri menargetkan bahwa data yang didapatkan merupakan data penting. Basis data merupakan kumpulan dari beberapa tabel yang terdiri dari beberapa *field* dan *field* yang terdiri dari beberapa kolom dan baris yang dapat digunakan untuk menyimpan sebuah data [1]. Tabel adalah matrik yang berisi data dan terlihat berbentuk *spreadsheet* sederhana, sedangkan kolom adalah satu elemen data terkandung dalam satu jenis data yang sama dan baris adalah sekumpulan data-data yang saling terhubung [2].

MySQL merupakan penerapan dari sebuah sistem manajemen basis data SQL yang bersifat terbuka dan gratis untuk digunakan berbagai pihak [3]. Sehingga MySQL banyak digunakan oleh banyak orang untuk penyimpanan data. Biasanya untuk merahasiakan isi teks basis data MySQL diterapkan penggunaan sandi. Yang menjadi masalah, jika data dari basis data MySQL dikirimkan kepada pihak yang disetujui maka diperlukan cara agar isi teks basis data MySQL tidak diketahui pencuri data.

Salah satu cara yang digunakan yaitu dengan merahasiakan isi teks basis data dengan teknik kriptografi. Kerahasiaan merupakan tindakan saat bertukar informasi dari sekelompok orang ataupun dapat juga satu orang dan menyembunyikannya dari orang yang tidak diberikan izin untuk mengetahuinya [4]. Kerahasiaan juga merupakan penjagaan privasi saat interaksi pada informasi yang diberikan dan juga informasi yang diterima sehingga pihak-pihak yang tidak terkait tidak dapat mengetahui isi informasi yang disampaikan dan di antara ilmu komputer juga terdapat kerahasiaan dalam menjaga sebuah data dan informasi sehingga data yang disimpan, dikelola maupun dikirim memiliki keamanan yang tidak diragukan [5]. Kriptografi merupakan ilmu yang diterapkan untuk merahasiakan sebuah pesan yang bersifat rahasia ataupun pribadi yang dilakukan oleh pihak-pihak yang berkaitan sehingga pihak-pihak yang tidak berkaitan tidak dapat mengetahui informasi yang bersifat rahasia tersebut dan umumnya pesan yang belum dirahasiakan biasanya disebut pesan asli (*plaintext*) dan pesan yang telah dirahasiakan disebut (*ciphertext*). [6]. Pesan asli (*plaintext*) merupakan sebuah teks biasa yang biasanya digunakan sebagai *input* untuk proses pada kriptografi dan pesan rahasia (*ciphertext*) merupakan pesan yang hanya dapat diketahui pihak yang telah menyepakati kerahasiaan pesan dan memiliki kunci kerahasiaan [7].

Penelitian yang berjudul desain enkripsi dan tanda tangan elgamal berbasis kisi skema menggunakan masalah SIS menyimpulkan bahwa kecurian dari sebuah data maupun informasi dapat diantisipasi dengan aman dan mudah [8].

Penelitian yang berjudul kriptografi *hybird* untuk file gambar menggunkan elgamal dan *double* algoritma

Diterima: 17-08-2019 | Revisi: 01-10-2019 | Diterbitkan: 03-10-2019 | DOI: 10.35134/jsisfotek.v1i1.11

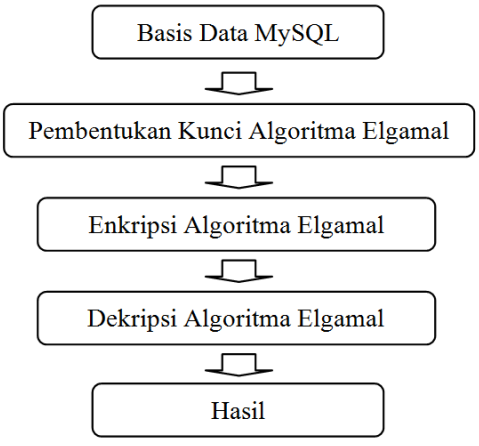
playfair ciper menyimpulkan bahwa *file* gambar yang dirahasiakan dapat memiliki keamanan yang lebih baik [9].

Penelitian yang berjudul skema otentikasi pengguna jarak jauh berbasis dua faktor menggunakan kriptografi elgamal menyimpulkan bahwa algoritma elgamal dapat digunakan untuk keamanan jenis apapun yang berbasiskan tulisan [10]. Penelitian yang berjudul analisis kombinasi algoritma elgamal dan algoritma LUC dalam keamanan file menyimpulkan bahwa keamanan file menjadi lebih baik [11].

Berdasarkan beberapa penelitian terdahulu yang menggunakan algoritma elgamal untuk menyelesaikan berbagai masalah kerahasiaan data, maka peneliti menggunakan algoritma elgamal untuk merahasiakan isi teks basis data MySQL. Algoritma elgamal merupakan sebuah algoritma yang dapat melakukan enkripsi dan dekripsi berdasarkan kunci asimetris yang artinya kunci *public* dan kunci *private* berbeda sehingga untuk melakukan proses enkripsi dan dekripsi juga dilakukan dengan jalan dan rumus yang berbeda [12]. Enkripsi merupakan teknik yang digunakan untuk merahasiakan teks ataupun data-data yang bersifat teks dan dekripsi merupakan teknik yang digunakan untuk membaca informasi [13]. Dengan adanya teknik kriptografi menggunakan algoritma elgamal maka isi teks basis data MySQL dapat dirahasiakan dari pencuri data.

2. Metodologi Penelitian

Metodologi penelitian pada penelitian ini meliputi beberapa tahapan yaitu menggunakan basis data MySQL, pembentukan kunci algoritma elgamal, enkripsi algoritma elgamal, dekripsi algoritma elgamal dan hasil. Gambar 1 adalah tahapan proses penelitian yang disusun berdasarkan tahapan awal hingga akhir penelitian.



Gambar 1. Tahapan Proses Penelitian

2.1. Basis Data MySQL

Basis data yang akan dirahasiakan adalah MySQL. Di dalam basis data MySQL terdapat tabel-tabel yang berisi teks dari data yang tersimpan. Teks dari data yang tersimpan akan dirahasiakan menggunakan algoritma elgamal.

2.2. Pembentukan Kunci Algoritma Elgamal

Pada algoritma elgamal untuk dapat mengenkripsi dan mendekripsi pesan dibutuhkan kunci *public* dan kunci *private*. Oleh karena itu untuk mendapatkan kunci *public* dan kunci *private* maka pada algoritma elgamal terlebih dahulu dilakukan pembentukan kunci dengan menentukan sembarang bilangan prima dan sembarang bilangan acak yang kemudian diproses sampai mendapatkan kunci *public* dan kunci *private*. Setelah mendapatkan dua kunci yaitu kunci *public* dan kunci *private*, maka kunci *public* digunakan untuk mengenkripsi pesan dan kunci *private* digunakan untuk mendekripsi pesan. Rumus pembentukan kunci *public* dan kunci *private* yaitu :

$y = g^x \bmod p$ ....(1)

Keterangan :

y : identitas kunci *public*

g : bilangan prima pertama

x : bilangan prima kedua

mod : sisa bagi

p : bilangan prima ketiga

Algoritma pembentukan kunci *public* dan kunci *private* disajikan pada Gambar 2.

```
Pseudo Code
Input: g, x, p
Output: y

  Initialization : primes
  if g = primes
    if x = primes
      if p = primes
        y =(g^x) mod p
      end if
    end if
end if
```

Gambar 2. Algoritma pembentukan kunci

Tahapan pembentukan kunci publik dan kunci privat yang dijelaskan sebagai berikut :

1. Gunakan Bilangan Prima (g)

   Bilangan prima (g) merupakan nilai pembentukan kunci pertama untuk mendapatkan kunci y.

2. Gunakan Bilangan Prima (x)

   Bilangan prima (x) merupakan nilai pembentukan kunci kedua untuk mendapatkan kunci y.

3. Gunakan Bilangan Prima (p)

   Bilangan prima (p) merupakan nilai pembentukan kunci ketiga untuk mendapatkan kunci y.

4. Hitung Nilai y

Setelah menentukan tiga bilangan prima yaitu g, x dan p maka tahapan selanjutnya menghitung nilai y.

5. Nilai y, g dan p Merupakan Kunci Publik.

   Setelah melakukan perhitungan nilai y maka didapatkan kunci publik yang digunakan untuk mengenkripsi teks. Kunci publik adalah y, g dan p.

6. Nilai x dan p Merupakan Kunci Privat.

   Setelah melakukan perhitungan nilai y maka didapatkan kunci privat yang digunakan untuk mendekripsi teks. Kunci privat adalah x dan p.

2.3. Enkripsi Algoritma Elgamal

Pada algoritma elgamal untuk melakukan enkripsi isi teks basis data MySQL, terlebih dahulu harus memiliki kunci untuk enkripsi yaitu kunci *public*. Setelah mendapatkan kunci *public* (y, g, p) yang digunakan untuk mengenkripsi teks. Rumus untuk mengenkripsi pesan yaitu :

Gamma :

$\gamma = g^k \bmod p$ ..... . (2)

Dimana :

γ : nilai gamma pembentuk *cipher* pertama

g : bilangan prima pertama

k : bilangan prima acak

mod : sisa bagi

p : bilangan prima ketiga

Delta :

$\delta = y^k.m \bmod p$ ..... .(3)

Dimana :

δ : nilai delta pembentuk *cipher* kedua

y : identitas kunci *public*

k : bilangan prima acak

m : nilai ASCII dari teks yang akan dirahasiakan

mod : sisa bagi

p : bilangan prima ketiga

Algoritma enkripsi teks disajikan pada Gambar 3.

Pseudo Code

```
Input: g, p, y, m
output: k, me, gamma, delta, cpr

  Initialization m, i
  Get length
    length=len(m)
    for i = 1 to length do
        k = Asc(Mid(k, i, 1)
        me = Asc(Mid(m, i, 1))
        gamma = g^k mod p
        delta = (y^k)*me mod p
        cpr = cpr & chr(gamma) & chr(delta)
    next
```

Gambar 3. Algoritma enkripsi

Tahapan proses enkripsi dijelaskan sebagai berikut :

1. *Plaintext*

   Plaintext yang akan dienkripsi adalah isi dari tabel basis data MySQL.

2. Ubah *Plaintext* Menjadi Kode ASCII Dan Susun Menjadi Blok-Blok Nilai m.

3. Menghasilkan Susunan Nilai m.

4. Tentukan Bilangan Acak k Sepanjang Jumlah *Plaintext*.

5. Menghasilkan Bilangan Acak k.

   Bilangan acak k yang telah dihasilkan akan digunakan sebagai pemangkat pesan.

6. Enkripsikan Setiap Blok m.

   Enkripsi setiap blok m dengan enkripsi Gamma dan Delta.

7. Menghasilkan *Ciphertext.*

   Satukan nilai gamma dan nilai delta sehingga menjadi *ciphertext.*

2.4. Dekripsi Algoritma Elgamal

Pada algoritma elgamal untuk melakukan dekripsi isi *ciphertext* basis data MySQL, terlebih dahulu harus memiliki kunci untuk dekripsi yaitu kunci *private* Setelah mendapatkan kunci *private* (x, p) yang digunakan untuk mendekripsi teks maka dapat dilakukan proses dekripsi. Rumus untuk mendekripsi pesan yaitu :

$m = \gamma.\delta\ (p\text{-}1\text{-}x) \bmod p$ ..... (4)

Dimana :

γ : nilai gamma pembentuk *cipher* pertama

δ : nilai gamma pembentuk *cipher* kedua

m : nilai ASCII dari teks yang akan dirahasiakan

x : bilangan prima kedua

mod : sisa bagi

p : bilangan prima ketiga

Algoritma dekripsi teks rahasia disajikan pada Gambar 4.

Pseudo Code

```
Input: p, x, m
output: gamma, delta, me, pln

  Initialization i
  Get length
    length=len(m)
    for i = 1 to length step 2 do
        gamma = Asc(Mid(m, i, 1)
        delta = Asc(Mid(m, i + 1, 1))
        me = (gamma * delta) * (p-1-x) mod p
        pln = pln & chr(me)
```

```
next
```

Gambar 4. Algoritma deskripsi

Tahapan proses enkripsi dijelaskan sebagai berikut :

1. *Ciphertext*

   Ambil *ciphertext* yang akan didekripsi menggunakan algoritma elgamal.

2. Pisahkan Nilai Gamma dan Delta Pada Pesan Rahasia (*Ciphertext*).

   Lakukan pemisahan urutan teks ganjil dan teks genap. Teks ganjil merupakan nilai gamma dan teks genap merupakan nilai delta.

3. Menghasilkan Nilai Gamma dan Delta

   Nilai gamma dan delta didapatkan setelah melakukan pemisahan dan disatukan dengan kelompok ganjil dan genap.

4. Konversi Nilai Gamma dan Delta Menjadi *Plaintext*

   Konversi nilai gamma dan delta menjadi *plaintext* Sehingga menghasilkan *plaintext* yang dihasilkan berupa m dalam desimal ASCII.

5. Menghasilkan *Plaintext*

   Lakukan penyusunan pesan m yang dihasilkan dan lakukan konversi karakter sehingga menjadi *plaintext.*

2.5. Hasil

Hasil yang didapatkan setelah melakukan proses pembentukan kunci dan proses enkripsi yaitu kerahasiaan isi teks basis data MySQL berupa *ciphertext* dan hasil yang didapatkan setelah melakukan proses dekripsi yaitu isi teks basis data MySQL yang telah dirahasiakan menjadi isi teks basis data MySQL yang asli berupa *plaintext.*

3. Hasil dan Pembahasan

Data yang digunakan untuk pengujian kerahasiaan teks basis data MySQL yaitu data *login* . Data ini digunakan sebagai uji coba untuk merahasiakan isi dari setiap tabel pada basis data MySQL. Algoritma yang digunakan untuk merahasiakan teks yang terdapat dalam tabel basis data yaitu Algoritma Elgamal. Data *login* berisi teks nama pengguna, sandi dan status. Teks yang terdapat pada *field password* akan dirahasiakan dengan algoritma elgamal dengan mengenkripsi teks di dalam tabel basis data MySQL. Untuk dapat merahasiakan sebuah teks maka di dalam algoritma elgamal diperlukan pembentukan dua buah kunci yaitu kunci *public* dan kunci *private*. Dimana masing-masing kunci memiliki fungsi yang berbeda, kunci *public* digunakan untuk mengenkripsi atau merahasiakaan teks basis data MySQL dan kunci *private* digunakan untuk mendekripsi teks atau mengembalikan kerahasiaan teks menjadi teks yang dapat dibaca. Data *login* yang isi dari *field* sandi akan dirahasiakan menggunakan algoritma elgamal dapat dilihat pada Tabel 1.

Tabel 1. Isi Teks Basis Data MySQL

Nama_pengguna	Sandi	Status
Admin	admin	Admin
Niko	nsa_st	Pengguna
Dino	dno_lk	Pengguna
Heni	hni_nv	Pengguna
Rahmayuni	rhm_ns	Pengguna
Ilham	ilh_tb	Pengguna
Bambang	bmb_rp	Pengguna
Secar	scr_123	Pengguna
Ana	ana_111	Pengguna
Anton	ant_pw	Pengguna
Faisal	fsl_000	Pengguna
Maulida	mld_ww	Pengguna
Saripah	srp_h1	Pengguna
M.Ali	m_ali	Pengguna
Tusim	tsm_ah	Pengguna

Berdasarkan Tabel 1 bahwa Teks Basis Data MySQL yang telah dijabarkan maka untuk merahasiakan teks dari *field* sandi dilakukan langkah dari algoritma elgamal.

Proses pembentukan kunci :

1. Bilangan prima yang digunakan adalah 127.
2. Bilangan acak pertama yang digunakan adalah 13.
3. Bilangan acak kedua yang digunakan adalah 17.
4. Hitung nilai y :

   $y = g^x \bmod p$

   $= 13^{17} \bmod 127$

   $= 44$

Sehingga diperoleh kunci *public* :

$y = 44$

$g = 13$

$p = 127$

Dan diperoleh kunci *private* :

$p = 127$

$x = 17$

Setelah mendapatkan kunci *public* dan kunci *private* tahap selanjutnya yaitu melakukan proses enkripsi menggunakan kunci *public* yaitu y, g dan p.

Proses Enkripsi:

Diketahui:

Plaintext : “admin”
Kunci *public* :
p = 127
g = 13
y = 44
Nilai k yang digunakan yaitu :
k1 = 11
k2 = 13
k3 = 17
k4 = 19
k5 = 23
Penyelesaian :
Ubah pesan asli (*plaintext*) ke dalam ASCII :
a=97
d=100
m=109
i=105
n=110
Sehingga nilai m adalah sebagai berikut :
m1 =97
m2 =100
m3 =109
m4 =105
m5 =110

Hitung gamma (γ) dengan rumus $\gamma = g^k \bmod p$
$\gamma 1 = 13^{11} \bmod 127$
$= 82$
$\gamma 2 = 13^{13} \bmod 127$
$= 15$
$\gamma 3 = 13^{17} \bmod 127$
$= 44$
$\gamma 4 = 13^{19} \bmod 127$
$= 70$
$\gamma 5 = 13^{23} \bmod 127$
$= 36$

Hitung delta dengan rumus $\delta = y^k .m \bmod p$
$\delta 1 = 44^{11} .97 \bmod 127$
$= 90$
$\delta 2 = 44^{13} .100 \bmod 127$
$= 98$
$\delta 3 = 44^{17} .109 \bmod 127$
$= 5$
$\delta 4 = 44^{19} .105 \bmod 127$
$= 28$
$\delta 5 = 44^{23} .110 \bmod 127$
$= 126$
Susun hasil perhitungan gamma (γ) dan delta (δ)
ASCII *Ciphertext* : 82, 90, 15, 98, 44, 5, 70, 28, 36, 126
Ubah ASCII *Ciphertext* menjadi karakter :
82 = R
90 = Z
15 =
98 =
44 = b
5 = ,
70 =
28 = F
36 = $
126 = ~
Ciphertext : RZ b, F $~

Setelah diimplementasikan pada seluruh data maka hasil enkripsi dapat dilihat pada Tabel 2.

Tabel 2. Data Uji Setelah Proses Enkripsi

Nama_pengguna	Sandi	Status
Admin	RZ b, F $~	Admin
Niko	R3 d,]FN$J)	Pengguna
Dino	RQ 9,KFN$`)G	Pengguna
Heni	RE 9,wFN$~)3	Pengguna
Rahmayuni	R' k, FN$~)D	Pengguna
Ilham	RB t,TFN$Y)z	Pengguna
Bambang	RW , FN$;)U	Pengguna
Secar	R$ @,5FN$d)G:	Pengguna
Ana	RZ 9,]FN$d)=Gq	Pengguna
Anton	RZ 9,{FN$)	Pengguna
Faisal	RK d,aFN$U)mGM	Pengguna
Maulida	R6 t,GFN$)	Pengguna
Saripah	R$ B,nFN$$)=	Pengguna
M.Ali	R6 7,]FV$3	Pengguna
Tusim	R! d, FN$:)X	Pengguna

Berdasarkan Tabel 2 teks basis data MySQL yang telah dijabarkan maka untuk merahasiakan teks dari *field* password dilakukan langkah dari algoritma elgamal berikut :

Proses Dekripsi :
Langkah-langkah penyelesaian proses dekripsi adalah sebagai berikut :

Diketahui :
Ciphertext : “RZ b, F $~”
Kunci *private* :
p=127
x=17

Penyelesaian :
Pisahkan nilai gamma dan delta pada pesan rahasia (*Ciphertext*).
γ = *Ciphertext* urutan ganjil.
δ = *Ciphertext* urutan genap.

Sehingga menjadi :
γ = R ,F$
δ = Zb ~

Ubah *Ciphertext* menjadi kode ASCII :
Nilai gamma :
γ1 = R = 82
γ2 = = 15
γ3 = , = 44
γ4 = F = 70
γ5 = $ = 36

Nilai delta :
δ1 = Z = 90
δ2 = b = 98

δ3 = = 5
δ4 = = 28
δ5 = ~ = 126
Hitung m (pesan asli) dengan rumus :
m = δ. γ (p-1-x) mod p.
Sehingga :
m1 = 82.90(127-1-17) mod 127
= 7390*109 mod 127
= 805510 mod 127
= 97
m2 = 15.98(127-1-17) mod 127
= 1470*109 mod 127
= 160230 mod 127
= 100
m3 = 44.5(127-1-17) mod 12
= 220*109 mod 127
= 23980 mod 127
= 109
m4 = 70.28(127-1-17) mod 127
= 1960*109 mod 127
= 213640 mod 127
= 105

m5 = 36.126(127-1-17) mod 127
= 4536*109 mod 127
= 494424 mod 127
= 110

ASCII *Plaintext* : 97, 100, 109, 105, 110

Ubah ASCII *Plaintext* menjadi karakter :
97 = a
100 = d
109 = m
105 = i
110 = n
Plaintext : "admin"

Uji coba dilakukan pada isi *field password* yang telah dirahasiakan pada tabel data *login*, maka hasil dari dekripsi algoritma elgamal dengan kunci *private* (p, x) = (127, 17) dapat dilihat pada Tabel 3.

Tabel 3. Data Uji Setelah Proses Dekripsi

Nama_pengguna	Sandi	Status
Admin	admin	Admin
Niko	nsa_st	Pengguna
Dino	dno_lk	Pengguna
Heni	hni_nv	Pengguna
Rahmayuni	rhm_ns	Pengguna
Ilham	ilh_tb	Pengguna
Bambang	bmb_rp	Pengguna
Secar	scr_123	Pengguna
Ana	ana_111	Pengguna
Anton	ant_pw	Pengguna
Faisal	fsl_000	Pengguna
Maulida	mld_ww	Pengguna
Saripah	srp_h1	Pengguna
M.Ali	m_ali	Pengguna
Tusim	Tsm_ah	Pengguna

4. Kesimpulan

Setelah melakukan tahapan proses penelitian mengenai kerahasiaan teks basis data MySQL menggunakan algoritma elgamal dapat disimpulkan bahwa algoritma elgamal dapat digunakan untuk merubah teks yang terdapat di dalam basis data MySQL menjadi teks rahasia (*ciphertext*) sehingga tidak dapat di baca oleh pencuri data.

Daftar Rujukan

[1] Warman, Sultan (2018). Perancangan Sistem Simulasi Data Terintegrasi (Studi Kasus : Data SIM, KTP dan KTM). *TEKNOIF*, 6(3), 100-109. https://doi.org/10.21063/JTIF.2018.V6.2

[2] Enterprise (2018). HTML, PHP dan MySQL Untuk Pemula. 1st ed. Bandung: *PT. Elex Media Komputindo.*

[3] Asaad, & Segerey (2017). School Management Application Using iOS. *Academic Journal of Nawroz University*, 7(4), 38-44. https://doi.org/10.25007/ajnu.v7n4a269

[4] Al-Zubi, M., & Abu-Shareha, A. A. (2019). Efficient signcryption scheme based on El-Gamal and Schnorr. *Multimedia Tools and Applications*, 78(9), 11091–11104. https://doi.org/10.1007/s11042-018-6636-7

[5] Dwork (2018). The Future Of The Journal Of Privacy And Confidentiality. *Journal of Privacy and Confidentiality*, 8(1), 1-2. https://doi.org/10.29012/jpc.708

[6] Ordonez, A. J., Gerardo, B. D., & Medina, R. P. (2018). Digital signature with multiple signatories based on modified ElGamal Cryptosystem. *5th International Conference on Business and Industrial Research (ICBIR), Bangkok*, 89-94. https://doi.org/10.1109/ICBIR.2018.8391172

[7] Kalsi, S., Kaur, H., & Chang (2018). DNA Cryptography and Deep Learning using Genetic Algorithm with NW algorithm for Key Generation. *Journal of Medical Systems*, 42(17). https://doi.org/10.1007/s10916-017-0851-z

[8] Gupta, D. S., & Biswas, G. P. (2017). Design of lattice-based ElGamal encryption and signature schemes using SIS problem. *Wiley Online Library*, https://doi.org/10.1002/ett.3255

[9] Hardi, S. M., Tarigan, J. T., & Safrina, N. (2017). Hybrid Cryptosystem For Image File Using Elgamal And Double Playfair Cipher Algorithm. Journal of Physics: Conference Series, 978(1), 012068. https://doi.org/10.1088/1742-6596/978/1/012068

[10] Soni, P., Ali, R., & Pal, A.K. (2017). A Two-factor based Remote User Authentication Scheme using ElGamal

Cryptosystem. *Proceedings of the ACM Workshop on Internet of Things (IoT) Security: Issues and Innovations*, Article No. 3. https://doi.org/10.1145/3084030.3084031

[11] Mawengkang, H., Siregar, A. F., & Efendi, S. (2018). Combination Analysis Of Elgamal Algorithm and LUC Algorithm In File Security. *IOP Conference Series: Materials Science and Engineering, Volume 420, conference 1*, https://doi.org/10.1088/1757-899x/420/1/012130

[12] Jannati, H., & Bahrak, B. (2017). An Oblivious Transfer Protocol Based on Elgamal Encryption for Preserving Location Privacy. *Wireless Personal Communications*, 97(2), 3113–3123 https://doi.org/10.1007/s11277-017-4664-7

[13] D. Rachmawati, A. S., Harahap, & Purba, R. N. (2018). A Hybird Cryptosystem Approach For Data Security By Using Triple DES Algorithm And Elgamal Algorithm. *IOP Conference Series: Materials Science and Engineering*, 453, 012018. https://doi.org/10.1088/1757-899x/453/1/012018