Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 721-727
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

# Three Pass Protocol untuk Keamanan Kunci Berbasis Base64 pada XOR Cipher

**Oris Krianto Sulaiman[1]*, Khairuddin Nasution[2], Mhd. Zulfansyuri Siambaton[3]**
Universitas Islam Sumatera Utara
Jl. Sisingamangaraja No.Kelurahan, Teladan Barat, Kec. Medan Kota, Kota Medan, Sumatera Utara 20217
*oris.ks@ft.uisu.ac.id

***Abstract***

*XOR cipher is a message randomization algorithm by performing XOR logical operations for plaintext and key so that it becomes a ciphertext. The problem lies in the predictable use of XOR. Therefore, it uses key security using the Three Pass Protocol. This protocol secures communication for each party. The key used for Three Pass Protocol communication is Base64. The Three Pass Protocol scheme for XOR Cipher key security using Base64 has a weakness because it is due to the Base64 encoding process which by default is easy for others to know. So that this research can be developed again to replace Base64 into a better algorithm in terms of security.*

***Keywords****: : XOR Cipher, Base64, Three Pass Protocol, Security Key.*

***Abstrak***

*XOR cipher merupakan algoritma pengacakan pesan dengan melakukan operasi logika XOR untuk plaintext dan kunci sehingga menjadi sebuah ciphertext. Permasalahan terletak pada penggunaan XOR yang mudah ditebak. Oleh sebab itu digunakan pengamanan kunci dengan menggunakan Three Pass Protocol. Protocol ini melakukan pengamanan komunikasi pada masing-masing pihak. Kunci yang digunakan untuk komunikasi Three Pass Protocol adalah Base64. Pada skema Three Pass Protocol untuk keamanan kunci XOR Cipher menggunakan Base64 memiliki kelemahan karena dikarenakan proses encoding Base64 yang secara default mudah diketahui oleh orang lain. Sehingga penelitian ini dapat dikembangkan kembali untuk mengganti Base64 menjadi algoritma yang lebih baik dari sisi keamanan.*

***Kata kunci****: XOR Cipher, Base64, Three Pass Protocol, Kemanan Kunci.*

## 1. PENDAHULUAN

Keamanan informasi menjadi perhatian penting pada saat ini, pertukaran informasi yang cepat di era digital membuat orang-orang dapat dengan mudah mendapatkan informasi. Informasi atau pesan yang saling berjalan di internet dapat diakses oleh siapa saja bahkan ketika anda menujukan sebuah pesan tersebut hanya kepada satu orang saja maka ada jutaan orang lain yang dapat melihat pesan tersebut, hal ini disebabkan karena internet dapat diakses oleh semua orang [1], [2]. Oleh sebab itu keamanan informasi atau pesan ini harus menjadi perhatian khusus agar pesan tersebut benar-benar aman dan tersampaikan kepada yang berhak menerima. Algoritma XOR Cipher merupakan salah satu algoritma kriptografi yang dapat digunakan untuk mengamankan pesan dengan memanfaatkan logika XOR. Namun algoritma XOR Cipher untuk penyandian memiliki kelemahan karena proses komputasi yang sederhana [3]–[5]. Oleh sebab itu untuk memperkuat keamanan pada XOR Cipher maka dapat

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 721-727
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

ditambahkan protokol komunikasi untuk mengamankan pertukaran kunci pada XOR Cipher. Salah satu protokol komunikasi yang dapat digunakan adalah Three Pass Protocol.

## 2. METODOLOGI PENELITIAN

### 2.1. XOR Cipher

Algoritma *Exclusive-OR* atau XOR Cipher merupakan algoritma kriptografi yang melakukan logika XOR untuk setiap binary dari text yang akan di enkripsi[6]. *Plaintext* beserta kunci akan di konversi menjadi biner untuk kemudian dilakukan proses XOR. Adapun tabel untuk XOR adalah sebagai berikut:

**Tabel 1.** Operasi *XOR*

| $p$ | $k$ | $c = p \oplus k$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

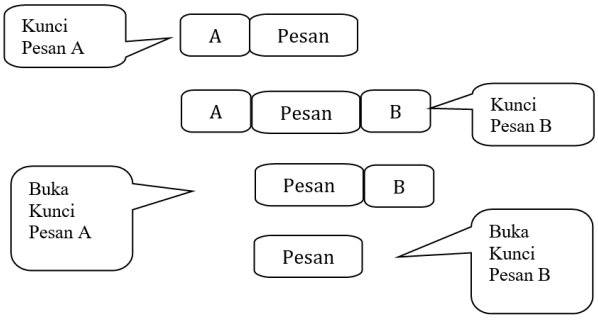
### 2.2. Base 64

Algoritma yang digunakan untuk melakukan proses *encoding* dan *decoding* bit yang terdapat dalam teks. Dalam tabel ASCII setiap satu karakter berisi 8bit bilangan biner. Base64 merupakan susunan gabungan antar setiap bit karakter kemudian disusun dengan pola 6bit berdasarkan tabel Base64[7]. Berikut contoh penggunaan Base64.

*Plaintext*: oris
*Encode* Base64: b3Jpcw==

### 2.3. Three Pass Protocol

Three Pass merupakan sebuah kerangka kerja pada proses komunikasi yang terjadi antara pengirim dan penerima pesan. Dalam proses komunikasi dengan menggunakan Three Pass akan memungkinkan si pengirim dan penerima pesan dapat melakukan komunikasi tanpa adanya kunci[8]. Three Pass Protocol melakukan langkah berikut untuk melakukan enkripsi (Enkripsi A – Enkripsi B – Dekripsi A – Dekripsi B)[9].




**Gambar 1.** Skema Three Pass Protocol

Pada penelitian ini metode yang digunakan untuk penyelesaian masalah adalah menggunakan encode kunci Base64 pada XOR cipher dengan Three Pass Protocol. Pada saat awal *plaintext* akan dikirim maka *plaintext* tersebut terlebih dahulu di enkripsi menggunakan XOR cipher sehingga menghasilkan *ciphertext* yang akan di *encode* menggunakan Base64. Hasil *encoding* ini akan menjadi kunci untuk proses pertukaran kunci pada Three Pass Protocol. Dalam XOR cipher jumlah karakter kunci yang digunakan untuk melakukan enkripsi terhadap *plaintext* harus sama panjangnya dengan jumlah *plaintext* tersebut. Berikut adalah rumus yang digunakan untuk enkripsi dan dekripsi XOR cipher.

$c = p \oplus k$

$p = c \oplus k$

dimana:

*p = plaintext*

*c = ciphertext*

*k = key*

Pada penelitian ini *plaintext* akan dikonversi menjadi *binner* yang berasal dari tabel ASCII untuk 26 karakter huruf berikut. Tabel I memperlihatkan karakter yang digunakan pada penelitian ini berjumlah 26 karakter.

**Tabel 2.** Tabel ASCII

| Index | Binary | Char | Index | Binary | Char |
|---|---|---|---|---|---|
| 0 | 01100001 | a | 13 | 01101110 | n |
| 1 | 01100010 | b | 14 | 01101111 | o |
| 2 | 01100011 | c | 15 | 01110000 | p |
| 3 | 01100100 | d | 16 | 01110001 | q |
| 4 | 01100101 | e | 17 | 01110010 | r |
| 5 | 01100110 | f | 18 | 01110011 | s |
| 6 | 01100111 | g | 19 | 01110100 | t |
| 7 | 01101000 | h | 20 | 01110101 | u |
| 8 | 01101001 | i | 21 | 01110110 | v |
| 9 | 01101010 | j | 22 | 01110111 | w |
| 10 | 01101011 | k | 23 | 01111000 | x |
| 11 | 01101100 | l | 24 | 01111001 | y |
| 12 | 01101101 | m | 25 | 01111010 | z |

Untuk mengamankan kunci maka dibuat sebuah text untuk *encoding* menggunakan *Base64* dengan nilai yang ada pada tabel 2. Sehingga akan menghasilkan binary 6bit untk masing masing karakter hasil *encoding* ini. Hasil ini akan digunakan untuk pertukaran kunci menggunakan Three Pass Protocol.

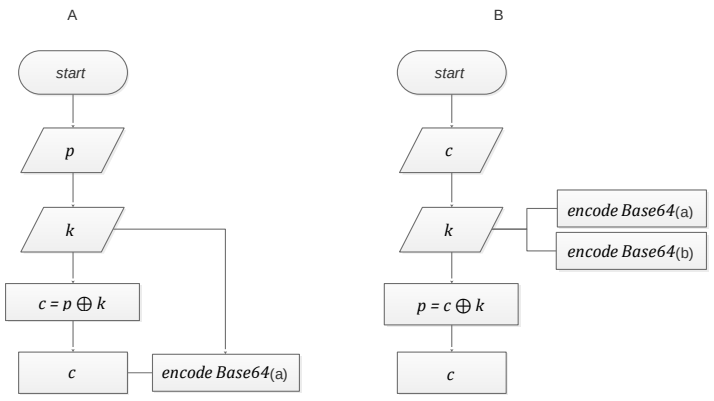
**Tabel 3.** *Base64 index*

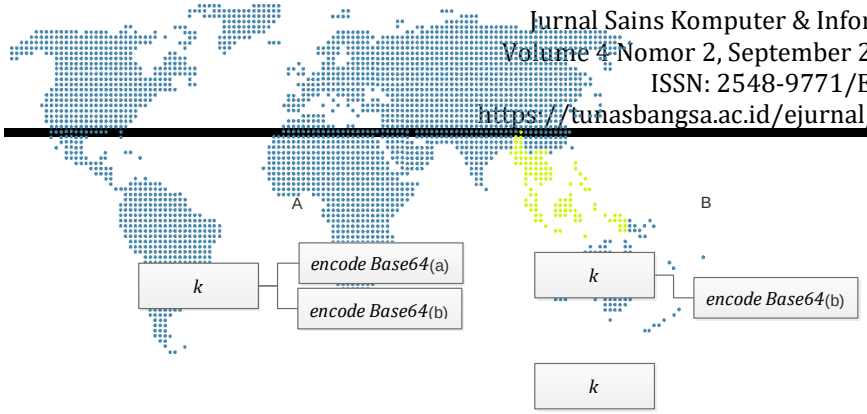
| Index | Binary | Char | Index | Binary | Char |
|---|---|---|---|---|---|
| 0 | 000000 | A | 33 | 100001 | h |
| 1 | 000001 | B | 34 | 100010 | i |
| 2 | 000010 | C | 35 | 100011 | j |

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 721-727
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

| Index | Binary | Char | Index | Binary | Char |
|---|---|---|---|---|---|
| 3 | 000011 | D | 36 | 100100 | k |
| 4 | 000100 | E | 37 | 100101 | l |
| 5 | 000101 | F | 38 | 100110 | m |
| 6 | 000110 | G | 39 | 100111 | n |
| 7 | 000111 | H | 40 | 101000 | o |
| 8 | 001000 | I | 41 | 101001 | p |
| 9 | 001001 | J | 42 | 101010 | q |
| 10 | 001010 | K | 43 | 101011 | r |
| 11 | 001011 | L | 44 | 101100 | s |
| 12 | 001100 | M | 45 | 101101 | t |
| 13 | 001101 | N | 46 | 101110 | u |
| 14 | 001110 | O | 47 | 101111 | v |
| 15 | 001111 | P | 48 | 110000 | w |
| 16 | 010000 | Q | 49 | 110001 | x |
| 17 | 010001 | R | 50 | 110010 | y |
| 18 | 010010 | S | 51 | 110011 | z |
| 19 | 010011 | T | 52 | 110100 | 0 |
| 20 | 010100 | U | 53 | 110101 | 1 |
| 21 | 010101 | V | 54 | 110110 | 2 |
| 22 | 010110 | W | 55 | 110111 | 3 |
| 23 | 010111 | X | 56 | 111000 | 4 |
| 24 | 011000 | Y | 57 | 111001 | 5 |
| 25 | 011001 | Z | 58 | 111010 | 6 |
| 26 | 011010 | a | 59 | 111011 | 7 |
| 27 | 011011 | b | 60 | 111100 | 8 |
| 28 | 011100 | c | 61 | 111101 | 9 |
| 29 | 011101 | d | 62 | 111110 | + |
| 30 | 011110 | e | 63 | 111111 | / |
| 31 | 011111 | f | Padding | | = |
| 32 | 100000 | g | | | |

Diagram alir dari proses Three Pass Protocol untuk keamanan kunci berbasis Base64 pada XOR Cipher ini dapat dilihat pada gambar berikut ini.






**Gambar 2.** Proses pertukaran kunci pada Three Pass Protocol

Pada saat awal pertukaran kunci, kunci awal akan di *encode* menggunakan Base64 untuk selanjutnya dikirim ke penerima pesan. *Ciphertext* pada saat awal ini tidak dapat dienkripsi karena kunci asli tidak diketahui. Kunci *base64* yang diterima di awal akan ditambahkan kembali dengan menggunakan *encoding* base64 (b) yang ditambahkan melalui proses acak oleh si penerima untuk kemudian dikembalikan lagi ke pengirim. Pengirim dalam hal ini akan *decoding* base64 sehingga kunci asli akan tampak namun kunci ini tetap akan dikirimkan bersamaan dengan kunci *base64* (b).

## 3. HASIL DAN PEMBAHASAN

Pada *plaintext* yang digunakan pada percobaan ini adalah "srie" dan kunci adalah "oris". Hasil dari XOR cipher dari penelitian ini merupakan binary dari *plaintext* srie ⊕ *key* oris seperti yang terlihat pada tabel berikut sehingga menghasilkan *ciphertext.*

**Tabel 4.** *XOR Cipher*

| ***Plaintext "srie"*** | ***Key "oris"*** | ***Ciphertext*** |
|---|---|---|
| 01110011 | 01101111 | 00011100 |
| 01110010 | 01110010 | 00000000 |
| 01101001 | 01101001 | 00000000 |
| 01100101 | 01110011 | 00010110 |

*Ciphertext* yang dihasilkan adalah: 00011100 00000000 00000000 00010110.

### 3.1. Pertukaran kunci Three Pass Protocol

Untuk pertukaran kunci awal maka yang perlu kita ketahui adalah kunci. Kunci = "oris". Kunci ini akan dikirimkan ke penerima namun akan dilakukan penambahan keamanan agar kunci tidak dapat diakses oleh orang lain. Pengirim akan membuat sebuah kata yang akan di *encoding* dalam hal ini pengirim menggunakan kata "arya" lalu di *encoding* dengan menggunakan base64 sehingga menjadi: YXJ5YQ== kunci "oris". Sehingga kunci "oris" mendapatkan keamanan YXJ5YQ==. Untuk melihat kunci asli maka harus *decoding* Base64 ini.

Ciphertext dikirimkan akan ditambahi kembali dengan menggunakan Base64 dari kata acak, pada contoh ini adalah "apik" sehingga mendapatkan

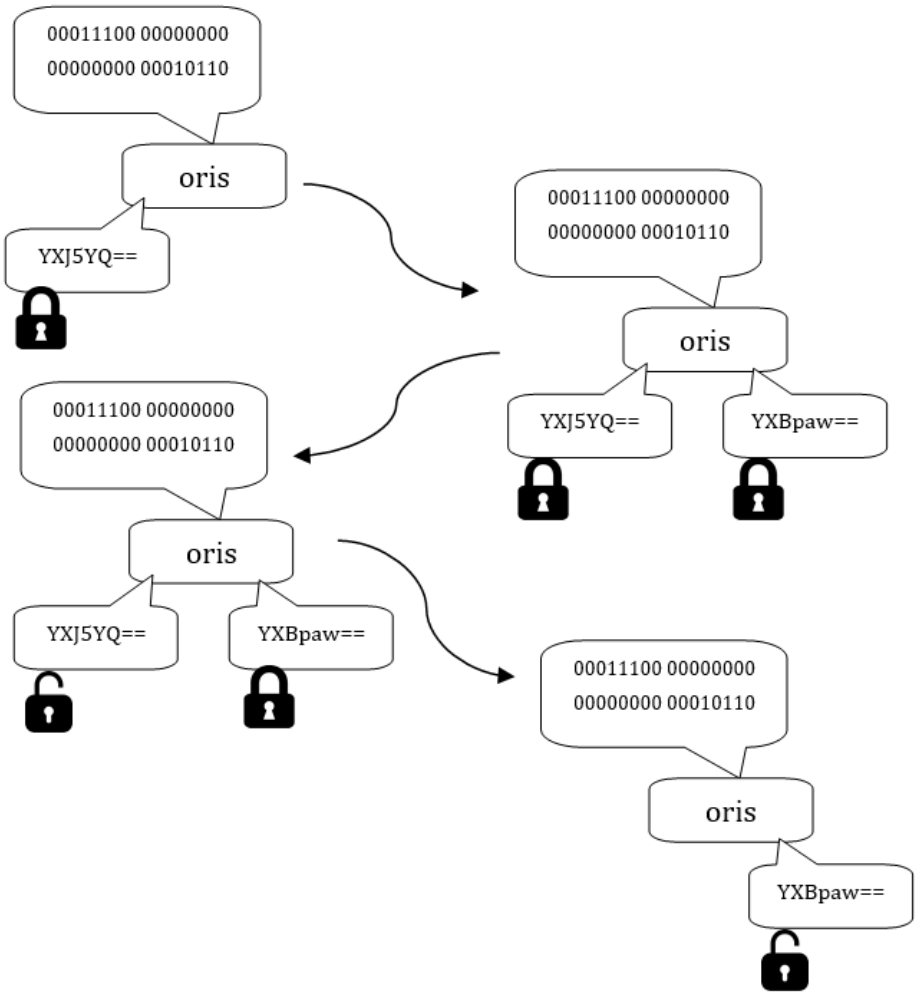
Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 721-727
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

hasil = YXBpaw==. Jadi kunci oris diamankan dengan dua base yaitu YXJ5YQ== dan YXBpaw==.

Pertukaran kunci kedua adalah penerima mengembalikan kembali kunci tersebut ke pengirim dan pengirim *decoding* Base64 yang dibuatnya diawal yaitu *decoding* YXJ5YQ== sehingga kunci tersisa adalah YXBpaw==.

Pertukaran kunci ketiga adalah pengirim akan mengirim kembali kunci dengan *encoding* sisa milik si penerima yaitu YXBpaw==. Karena *encoding* ini milik penerima maka dapat di *decode* oleh si penerima karena penerima yang membuat kunci ini. Setelah base64 milik penerima di *decode* maka kunci sudah tidak memiliki keamanan dan dapat dilihat oleh si penerima.

Berikut ini adalah gambaran pertukaran kunci basis Base64 pada XOR Cipher.




**Gambar 3.** Proses pengiriman pesan dan kunci

Pada gambar 3 merupakan pengiriman pesan *ciphertext* dari XOR cipher dan terlihat kunci di *encode* menggunakan Base64.

## 4. SIMPULAN

Pesan yang dienkripsi dengan menggunakan XOR cipher sangat rentan dibobol jika kunci diketahui oleh kriptanalis, oleh sebab itu pengamanan terhadap kunci tersebut juga harus diperhatikan. Dengan menggunakan Three Pass Protocol maka pertukaran kunci akan mendapatkan keamanan berlapis sehingga kunci tidak mudah diketahui. Base64 disini dapat diganti dengan menggunakan algoritma lainnya agar menambah keamanan pada saat pertukaran kunci. Karena sifatnya Base64 mudah di *encoding* dan *decoding* sehingga pengembangan lanjutan dapat menggunakan algoritma kriptografi pada saat pertukaran kunci Three Pass Protocol.

## DAFTAR PUSTAKA

[1] A. P. Galih, "Keamanan Informasi (Information Security) Pada Aplikasi Perpustakaan IPusnas," *AL Maktabah*, vol. 5, no. 1, p. 10, 2020, doi: 10.29300/mkt.v5i1.3086.

[2] I. Darmayanti, D. N. Astrida, and D. Arius, "Penerapan Keamanan Pesan Teks Menggunakan Modifikasi Algoritma Caisar Chiper Kedalam Bentuk Sandi Morse," *Jurnal IT CIDA*, vol. 4, no. 1, pp. 39–47, 2018.

[3] O. Krianto Sulaiman, "Hybrid Cryptosystem Menggunakan Xor Cipher Dan Merkle-Hellman Knapsack Untuk Menjaga Kerahasiaan Pesan Digital," *Jurnal Teknologi Informasi*, vol. 3, no. 2, pp. 169–173, 2019.

[4] J. H. Lubis, "Implementasi Keamanan Data Dengan Metode Kriptografi XOR," *Jurnal Sistem Informasi Kaputama (JSIK)*, vol. 2, no. 2, pp. 1–4, 2018.

[5] R. Amalia and P. Rosyani, "Implementasi Algoritma AES dan Algoritma XOR pada Aplikasi Enkripsi dan Dekripsi Teks Berbasis Android," *Faktor Exacta*, vol. 11, no. 4, p. 370, 2018, doi: 10.30998/faktorexacta.v11i4.2878.

[6] Suhardi, "Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-or (Xor)," *Jurnal Teknovasi*, vol. 03, no. 2, pp. 23–31, 2016.

[7] O. K. Sulaiman, K. Nasution, and S. Y. Prayogi, "Base64 Sebagai Kunci Keamanan pada One Time Pad (OTP)," *CESS (Journal of Computer Engineering, System and Science)*, vol. 5, no. 2, p. 241, 2020, doi: 10.24114/cess.v5i2.19622.

[8] S. Prayudi *et al.*, "Analisis keamanan pada kombinasi protokol secret sharing dan three-pass," vol. IV, no. 2, pp. 1–6, 2015.

[9] B. Oktaviana and A. P. Utama Siahaan, "Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography," *IOSR Journal of Computer Engineering*, vol. 18, no. 04, pp. 26–29, 2016, doi: 10.9790/0661-1804032629.