Analisis dan Perbandingan Keamanan pada Wireless LAN dengan Enkripsi AES (*Advanced Encryption Standard*) dan TKIP(*Temporal Key Inegrity Protocol*)

Abdurrisyad Fikri - 13508017
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18017@students.if.itb.ac.id, abdurrisyadfikri@yahoo.com

***Abstract*—Pada zaman sekarang, penggunaan jaringan komputer sudahlah sangat luas. Salah satunya adalah penggunaan jaringan nirkabel pada jaringan komputer lokal atau yang biasa disebut dengan WLAN (Wireless LAN). Maraknya penggunaan teknologi ini di berbagai tempat membuat banyaknya data atau informasi yang mengalir dalam jaringan ini yang tentu saja di saat atau kondisi tertentu harus diproteksi dari orang-orang yang tidak berhak untuk mengakses data atau informasi tersebut. Hal ini menyebabkan algoritma enkripsi untuk menyamarkan data ataupun melindungi hak akses ke data tersebut menjadi sangat penting. Berdasarkan standar untuk produk-produk Wi-Fi, terdapat beberapa protokol untuk mengamankan Wi-Fi dari berbagai serangan. Protokol enkripsi yang lazim dipakai adalah WEP dan WPA dimana WEP sudah banyak tergantikan oleh WPA, dan algoritma enkripsi yang populer digunakan dalam protokol WPA adalah TKIP dan AES yang akan dibahas pada makalah ini. Pada makalah ini akan dibahas tentang cara kerja kedua algoritma ini dan kemungkinan celah-celah keamanan yang mungkin terdapat dalam kedua algoritma ini dalam pengimplementasiannya untuk keamana WLAN.**

***Index Terms*—WLAN, Wi-Fi, WEP, WPA, TKIP, AES**

I. PENDAHULUAN

Pada pertengahan abad 20, pemanfaatan teknologi pengiriman informasi dengan menggunakan gelombang radio berkembang pesat. Pada awalnya kebutuhan akan keamanan pada transfer hanya dibutuhkan oleh kalangan militer, namun seiring berkembang pesatnya teknologi ini yang ikut memicu turunnya harga dari penggunaan teknologi ini, pemakaian teknologi inipun meluas hingga akhirnya seperti keadaan sekarang. Saat ini penggunaan jaringan komputer nirkabel sangat banyak mulai dari rumah, kantor, mall, rumah sakit, kampus, dsb.

Walaupun teknologi nirkabel untuk komputer ada banyak jenisnya, seperti *bluetooth, Home RF*, dsb, teknologi yang paling populer untuk digunakan pada area yang terbatas (lokal) adalah Wi-Fi (Wireless Fidellity). "Wi-Fi" adalah nama (brand) yang dikeluarkan oleh Wi-Fi Alliance. Tujuan dari pemberian nama (brand) tersebut adalah untuk mengidentifikasi produk yang telah menjalani tes untuk meyakinkan *interoperability* (kemampuan beroperasi antar *device*) antar vendor yang ada. Produk-produk Wi-Fi harus dirancangn mengikuti standar industri yang dikenal dengan nama IEEE 802.11.

Lalu mengapa keamanan dari jaringan Wi-Fi perlu benar-benar diperhatikan? Tidak seperti jaringan kabel biasa, jaringan nirkabel sangat rentan untuk dimasuki oleh orang-orang yang tidak berkepentingan. Bukan hanya orang yang tidak mempunyai kepentingan/hak dapat mengambil informasi yang ada pada jaringan tersebut, orang pun dapat menanamkan data berbahaya, virus misalnya, yang dapat merusak dan menghancurkan informasi dan data yang ada.

Lalu bagaimana cara mengamankannya? Terdapat dua buah protokol yang (pernah) dikenal dalam dunia jaringan nirkabel, keduanya ini tentu dikembangkan menurut standar yang telah ditetapkan oleh IEEE. Protokol yang pertama adalah WEP (*Wired Equivalent Privacy*). Protokol ini menggunakan algoritma enkripsi RC4 dengan kunci 64-bit dalam pengimplementasiannya. Protokol ini hanya bertahan selama lima tahun sejak dikenalkan. Pada tahun 2001 ditemukan kakas untuk menjebol (crack) protokol ini dalam waktu singkat.

Protokol yang kedua adalah WPA (Wi-Fi Protected Access). Protokol ini dikembangkan untuk memperbaiki WEP yang telah "gagal dalam menjalankan tugasnya". Algoritma yang diterapkan pertama kali adalah TKIP (*Temporal Key Integrity Protocol*) yang sebenarnya adalah perbaikan dari algoritma WEP sebelumnya dengan menambahkan beberapa elemen yang dapat memperkuat algoritma tersebut dari serangan-serangan yang biasa dilancarkan pada sekuritas jaringan nirkabel.

Algoritma kedua yang populer digunakan dalam protokol ini adalah AES (*Advanced Encryption Standard*) atau Algoritma Rijndael. Algoritma ini adalah algoritma yang berbasis padaenkripsi blok *cipher*.

Penjelasan mengenai teori enkripsi, cara kerja algoritma-algoritma diatas, mengapa algoritma tersebut digunakan, dan algoritma manakah yang lebih baik untuk digunakan pada jaringan nirkabel (WLAN) akan dibahas pada bab-bab berikutnya.

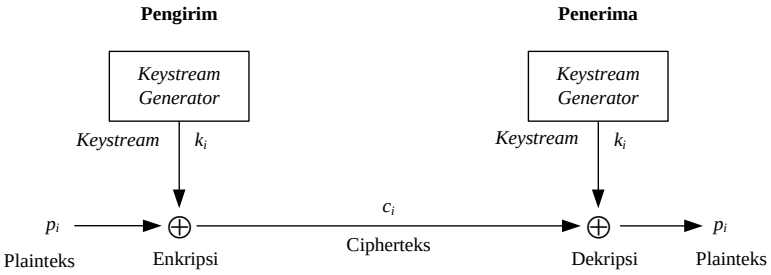
II. PENEJALASAN

TEORI ALGORITMA ENKRIPSI MODERN

Algoritma yang digunakan pada protokol-protokol pengamanan seperti yang disebutkan sebelumnya adalah termasuk algoritma enkripsi modern karena keduanya beroperasi pad mode bit, yaitu algoritma RC4 yang berbasis enkripsi cipher aliran (*stream cipher*) dan AES yang berbasis enkripsi cipher blok (*block cipher*). Berikut penjelasan menganai kedua jenis enkripsi tesebut.

A. *Cipher* Aliran (*Stream Cipher*)

Pada kategori enkripsi ini, enkripsi dilakukan pada bit tunggal, dan dioperasikan bit per bit atau byte per byte . *Plaintext* dienkripsi menjadi menjadi *ciphertext* dengan satu bit setiap transformasi ataupun satu byte setiap transformasi dengan mengunakan keystream. Algoritma ini diperkenalkan oleh Vernam pada algoritmanya **Vernam Cipher.** Berikut ilustrasi dari enkripsi menggunakan ciper aliran.



Pada jenis enkripsi ini, bit-bit kunci untuk enkripsi disebut *keystream*, *keystream* dibangkitkan oleh *keystream generator*. Setiap bit dari *plaintext* dienkripsi (misal dengan operasi XOR ⊕) dengan bit dari *keystream* dengan formula seperti ini

$$c_i = p_i \oplus k_i$$

dimana c_i adalah bit *ciphertext*, p_i adalah bit *plaintext* k_i adalah bit *key*. Lalu pada sisi penerima, *ciphertext* didekripsi kembali dengan menggunakan pola formula yang sama, yaitu

$$p_i = c_i \oplus k_i$$

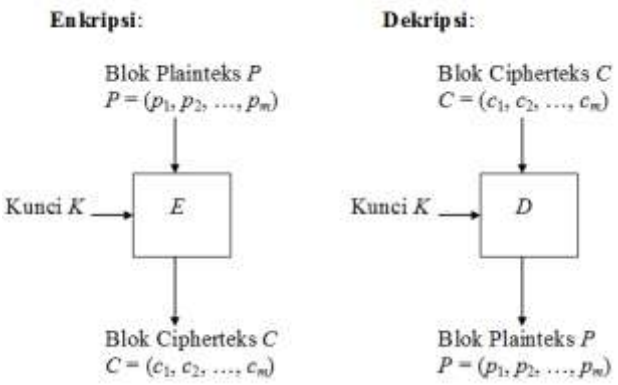
contoh dari operasi diatas adalah sebagai berikut

Plainteks:	1100101
Keystream:	1000110 ⊕
Cipherteks:	0100011

Keamanan dari sistem cipher aliran ini baregantung sepenuhnya pada *keystream generator.*

B. *Cipher* Blok (*Block Cipher*)

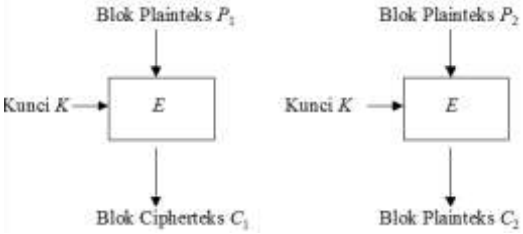
Pada jenis enkripsi ini, plain teks dienkripsi per blok-blok bit dengan panjang yang sama, misalnya 64- bit. Panjang kunci yang digunakan sama dengan panjang dari tiap blok. Panjang blok *ciphertext* yang dihasilkan akan sama dengan panjang blok *plain text.*



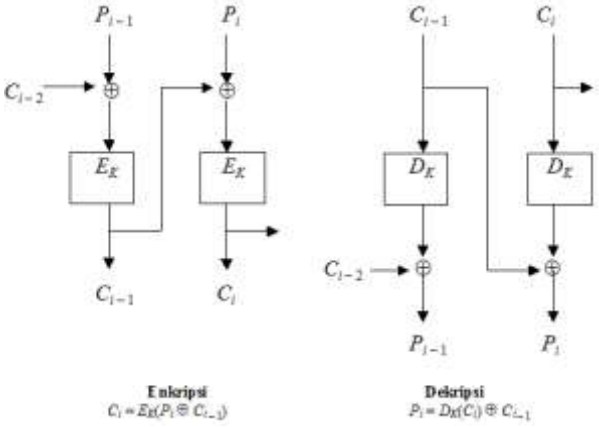
Gambar diatas adalah ilustrasi umum enkripsi dan dekripsi dengan menggunakan sistem *cipher block.*

Dalam penggunaan sistem ini , terdapat empat jenis mode operasi yang dapat digunakan yaitu :

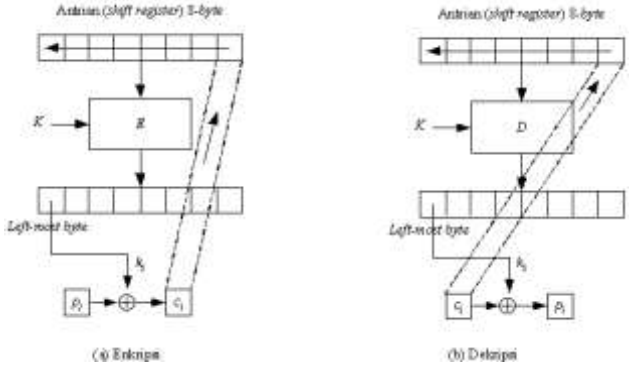
1. *Electronic Code Book* (ECB)
   pada mode ini, setiap blok dieksekusi secara independen.



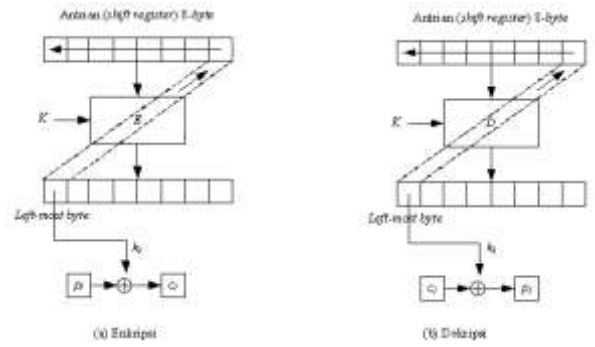
2. *Cipher Block Chaining* (CBC)
   Pada mode ini, cipher block tidak hanya bergantung padablok plainteks nya, namun jugapada seluruh blok plainteks sebelumnya.



3. *Cipher FeedBack* (CFB)



4. *Output FeedBack*(OFB)



(a) Enkripsi (b) Dekripsi

III. PENJELASAN TENTANG WEP

WEP (*Wireless Equivalent Privacy*) adalah algoritma standar untuk digunakan pada wireless LAN yang tedapat pada standar IEEE 802.11. Algoritma ini mempunya tiga buah goal, yaitu

1. Mencegah penyingkapan paket pada saat pengiriman (transit)
2. Mencegah modifikasi paket pada saat transit
3. Menyediakan *access control* untuk penggunaan jaringan.

Pada dasarnya algoritma untuk WEP ini menggunakan algoritma RC4. RC4 adalah algoritma *stream cipher*, algoritma ini memproses data dalam ukuran byte bukan bit, untuk membangkitkan *keystream*, *cipher* menggunakan status internal yant terdiri dari :

– Permutasi angka 0 sampai 255 di dalam larik S_0, S_1, …, S_{255}. Permutasi merupakan fungsi dari kunci *U* dengan panjang variabel.
– Dua buah pencacah indeks, *i* dan *j*

Berikut sistematika algoritma RC4 secara umum:

1. Inisialisasi larik *S*: $S_0 = 0$, $S_1 = 1$, …, $S_{255} = 255$

```
for i ← 0 to 255 do
  S[i] ← i
endfor
```

2. Jika panjang kunci *U* < 256, lakukan *padding* sehingga panjang kunci menjadi 256 *byte*.

Contoh: *U* = "abc" (3 *byte*)
Padding: *U* = "abcabcabc…" sampai panjang *U* mencapai 256 *byte*

3. Lakukan permutasi nilai-nilai di dalam larik *S* :

```
j ← 0
for i ← 0 to 255 do
  j ← (j + S[i] + U[i]) mod 256
  swap(S[i], S[j])
endfor
```

4. Bangkitkan aliran-kunci dan lakukan enkripsi:

```
i ← 0
j ← 0
for idx ← 0 to PanjangPlainteks – 1 do
  i ← (i + 1) mod 256
  j ← (j + S[i]) mod 256
  swap(S[i], S[j])
  t ← (S[i] + S[j]) mod 256
  K ← S[t]        (* keystream *)
  c ← K ⊕ P[idx]
endfor
```

Pada WEP terdapat dua istilah yaitu WEP Key dan WEP Seed. Terdapat dua jenis WEP Key yaitu 40bit atau 140bit yang digunakan sebagai kunci dasar bagi setiap paket. Ketika dikombinasikan dengan Initialization Vector (IV) 24bit yang akan selau di-generate agar selalu unik karena RC4 adalah algoritma *stream cipher*, kunci ini menjadi WEP seed. WEP Seed adalah 64bit atau 128bit. WEP Seed ini yang kemudian dijadikan kunci bagi RC4.

Lalu untuk mencegah paket dimodifikasi ketika transit, algoritma ini menambahkan ICV (*Integrity Check Value*) sepanjang 4 byte yang di enkripsi bersama-sama dengan paket dengan menggunakan RC4 yang berfungsi seperti *checksum.*

Berikut adalah algoritma untuk melakukan penjadwalan kunci pada WEP

```
Key Scheduling Algorithm (Key, Length)

    Key: array[Length] of int8

    Length: int8    # length of the key

    # Fill the S-box with values 0 to
255

    for i := 0 to 255

        S[i] := i

    end for

    # Scramble the S-box using the Key

    j := 0

    for i := 0 to 255

        j := ( j + S[i] + Key[i mod
Length] ) mod 256

        swap (S[i], S[j])

    end for

end Key Scheduling Algorithm
```

Lalu berikut adalah algoritma untuk men-generate kunci *pseudorandom*

```
Pseudorandom Generation Algorithm (Length)

   Length: integer # length of the
Keystream needed

   Keystream[]: array of int8

   i := 0

   j := 0

   for k := 0 to Length - 1
```

```
        i := (i + 1) mod 256

        j := (j + S[i]) mod 256

        swap (S[i], S[j])

        # Generate one byte of the
keystream

        Keystream[k] := S [ (S[i] + S[j] )
mod 256 ]

    end for

    return Keystream

end Pseudorandom Generation Algorithm
```

Seperti yang telah dipaparkan sebelumnya, algoritma WEP ini ternyata memiliki celah yang berhasil membuat algoritma ini gagal dalam lima tahun, yaitu adanya kemungkinan terjadinya *collision* dalam *generate* nilai IV sehingga dapat dimanfaatkan oleh pihak yang ingin menjebol, selain itu pada pemakaian ICV, letak ICV pada paket selalu tetap sehingga *hacker/cracker* dapat mengubah isi paket tanpa mengubah nilai ICV karena *stream cipher* dieksekusi per bit, maka *hacker* hanya perlu mengubah sampai bit sebelum ICV.

IV. PENJELASAN TENTANG WPA

Pada bab sebelumnya telah dijelaskan bahwa protokol WEP tidak lagi dapat diandalkan untuk mengamankan jaringan nirkabel (WLAN) dengan baik. Untuk mengatasi hal ini, maka dirancanglah protokol baru (lebih tepatnya diperbarui) yang dapat mengatasi kelemahan-kelemahan WEP. Protokol baru ini diberi nama WPA (Wi-Fi Protected Access). Pada pengembangan awal protokol ini, algoritma yang digunakan adalah perbaikan dari protokol WEP yaitu RC4 namun telah diimprovisasi untuk mengatasi celah-celah yang telah disebutkan sebelumnya. Improvisasi ini dilakukan, tidak langsung mengganti dengan yang baru, untuk menyeseuaikan dengan *device-device* lama yang telah memakai WEP agar pengguna tidak merasa "kaget". Lalu pada pengembangan berikutnya dirancanglah protokol yang menggunakan algoritma yang benar-benar baru yaitu algoritma AES (Rijndael Algorithm). Berikut penejelasan tentang protokol-protokol tersebut :

A. Temporal Key Integrity Protocol (TKIP)/(802.11i/WPA)

TKIP adalah protokol yang dirancang untuk membenahi celah-celah yang ada di WEP dan juga harus dapat menyesuaikan dengan hardware-hardware yang sebelumnya menggunakan WEP. Untuk mengatasi masalah-masalah tersebut, TKIP mengimplementsikan tiga buah protokol, yaitu :

1. Algoritma kriptografi untuk *message integrity* atau yang biasa disebut dengan MIC (*Message Integrity Check*) atau Michael, untuk mencegah modifikasi pada paket (ICV).
2. Algoritma *Key Mixing* (*Key Mixing Algorithm*), dan
3. Perbaikan pada initialization vector (IV)

Seperti yang telah disebutkan, penggunaan MIC adalah untuk mengatasi masalah pada ICV, maka MIC mengguanakan suatu algoritma hash untuk menghasilkan semacam *checksum* yang disebut *Michael Algorithm* yang menggunakan *padded MSDU* sebagai masukannya. MSDU adalah singkatan dari *MAC Service Data Unit* yaitu informasi mendasar dari paket yang akan dikirim. *Padded MSDU* tidak ditransmisikan melainkan hanya digunakan oleh Michael. Berikut algoritma dari Michael

```
Michael (Key, MSDU)

    Key: array[2] of int32

    MSDU: array [Length] of int32

    Length: integer         # length of the
padded MSDU in 32-bit words

    left := Key[0]; right := Key[1]

    for i := 0 to (n-1):

        left := left XOR MSDU[i]

        (left, right) := Block (left,
right)

    end for

    return (left, right)

end Michael

Block() is defined as:

Block (left, right)

    left, right: int32

    right := right XOR (left << 17)

    left := (left + right) MOD 2^32

    right := right XOR (XSWAP(left))

    left := (left + right) MOD 2^32

    right := right XOR (left << 3)

    left := (left + right) MOD 2^32

    right := right XOR (left >> 2)

    left := (left + right) MOD 2^32

    return (left, right)

end Block
```

Mekanisme kedua yang digunakan adalah dengan menggunakan TSC(*TKIP Sequence Counter*) untuk menggantikan IV. TSC adalah counter 48bit yang dimulai pada 0 dan ditambah 1 di setiap paketnya.

Lalu mekanisme ketiga adalah dengan menggunakan *Key Mixing Algorithm*, yaitu algoritma yang dirancang untuk melindungi TEK (*Temporal Encryption Key*) yaitu kunci yang dapat diganti-ganti dengan menggunakan *key management* (tidak dibahas disini). *Key Mixing Algorithm* mengombinasikan TEK dengan TSC dan *Transmitter Address*(TA) untuk membuat paket yang unik, 128bit WEP Seed, yang digunakan dalam WEP.

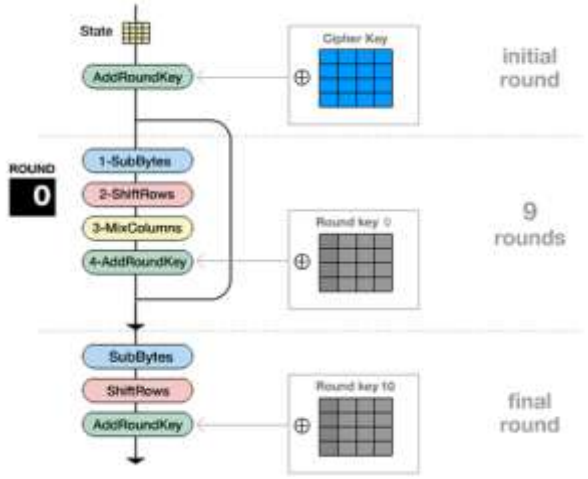
B. AES (*Advanced Encryption Standard*)

Algoritma Rijndael atau yang populer dengan sebutan AES adalah algorima enkripsi simetri dengan basis *block cipher*. AES memiliki tiga varian yaitu AES-128bit, AES-192bit, AES-256bit, namun yang paling sering digunakan adalah AES 128-bit dan AES-256bit, dan yang lazim dipakai pada sekuritas Wi-Fi adalah AES dengan panjang kunci dan blok 128bit.

Garis besar algoritma ini adalah sebagai berikut :

1. *AddRoundKey*, yaitu menambahkan (XOR) blok plainteks dengan blok *cipher key*
2. Putaran sebanyak *Nr*-1 kali yang terdiri dari :
   - SubBytes:substitusi byte dengan menggunakan S-Box
   - ShiftRows:Pergeseran baris-baris array secara wrapping
   - MixColumns: Mengacak data yang ada di masing-masing kolom *array state*
   - AddRoundKey: melakukan XOR antara state dengan RoundKey
3. Final Round: SubBytes, ShiftRows, dan AddRoundKey

Ilustrasi dari urutan jalannya algoritma diatas dapat dilihat pada gambar dibawah ini :



Pada AES yang menjadi salah satu pokok kekuatan algoritmanya adalah panjang kunci nya yaitu 128 bit, sehingga terdapat 2^{128} atau $2{,}4 \times 10^{38}$ kemungkinan kunci. Selain itu, perputaran sejumlah *Nr*-1 kali yang didalamnya terdapat proses substitusi (dengan S-Box) dan transposisi baris dan kolom (ShiftRows dan MixColumns) serta masih ditambah dengan XOR dengan kunci yang digenerate dengan algoritma *KeySchedule* menjadikan algoritma ini begitu kuat.

Berbeda dengan TKIP yang harus menyesuaikan dengan WEP yang sudah terdapat celah-celah kegagalannya, AES dirancang dari awal dan memang ditujukan untuk device yang baru yang belum menggunakan WEP, oleh karena itu algoritma ini tidak membawa "beban bawaan".

V. ANALISIS PERBANDINGAN KEAMANAN

Seperti yang telah dikemukakan diawal, makalah ini hanya membahas perbandigan keamanan antara algoritma TKIP dan AES, berdasarkan hasil analisis pada cara kerja kedua algoritma diatas, dan pengujian yang mampu dilakukan selama penyusunan makalah ini, dihasilkan hasil sebagai berikut :

1. Berdasarkan cara kerja TKIP, yang merupakan pengembangan WEP, masih terdapat celah yang dapat dimanfaatkan oleh penyerang (*attacker*) pada jaringan, yaitu dengan mencoba mengambil nilai dari IV. Walaupun IV telah dimodifikasi dengan menggunakan TSC, jika *attacker* berhasil "menangkap" paket sebelum sampai ke tujuan, *attacker* dapat mengganti paket tersebut dengan paket yang salah dengan IV yang lebih besar dibandingkan TSC, sehingga membuang paket tersebut dan *attacker* juga dapat memperoleh MSDU nya.
2. AES memiliki struktur yang lebih kuat dibandingkan TKIP karena tidak menyertakan data-data sensitif seperti TKIP yang dapat "ditangkap" oleh attacker, satu-satunya cara saat ini yang dapat digunakan untuk menjebol algoritma ini adalah dengan *brute force*, namun daya yang dikeluarkan dapat melebihi nilai informasi yang ditangkap.
3. Pada pengujian pada WLAN dengna menggunakan router untuk rumahan/jangkauan kecil (N-Lite Router), kedua algoritma berfungsi dengan baik, dan belum berhasil dijebol/dipatahkan.
4. Penggunaan AES saat ini lebih dominan karena pada produk-produk Wi-Fi baru sudah mulai men-support penggunaan AES dan "meninggalkan" TKIP

5. Penggunaan kunci pada implementasi AES pada device Wi-Fi yang diuji lebih fleksibel dibandingkan TKIP

Berdasarkan hasil studi literatur (bukan analisis mauapun pengujian pribadi), telah terdapat sekelompok orang yang berhasil "menyerang" keamanan WLAN yang menggunakan sistem/protokol WPA/TKIP.

VII. KESIMPULAN

1. AES lebih aman digunakan untuk pengamanan WLAN (Wi-Fi) baik untuk sekala besar maupun kecil.
2. TKIP masih aman digunakan untuk jaringan sekala kecil, misalnya rumah, sekolah, dll.
3. TKIP mempunyai potensi untuk dipatahkan lebih besar dibandingkan dengan AES.
4. Implementasi AES mulai menggeser penggunaan TKIP pada *device-device* baru.

REFERENSI

[1] Munir, Rinaldi. *Bahan Kuliah IF3058*.2009. Program Studi Teknik Informatika. Institut Teknologi Bandung.

[2] Edney, John. William A. Arbaugh. *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*.2003.Addison Wesley

[3] http://www.iphelp.ru/doc/3/Cisco.Press,.Cisco.Wireless.LAN.Security.%282004%29.DDU/1587051540/ch08lev1sec2.html

[4] B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.

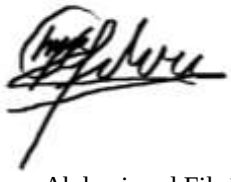
[5] http://www.5starsupport.com/tutorial/wireless-security.html

[6] http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011



Abdurrisyad Fikri
13508017