PROSIDING
Seminar Nasional MIPA 2016
Naskah diseminarkan pada 5 November 2016 dan dipublikasikan pada
http://conf.unnes.ac.id/index.php/mipa/mipa2016/schedConf/presentations

Differential Attack pada Algoritma PRESENT

Sandromedo Christa Nugroho[1] dan Wahyu Indah Rahmawati[2]
Lembaga Sandi Negara
email: sandromedo.christa@lemsaneg.go.id[1], wahyu.indah@lemsaneg.go.id[2]

Abstrak

Pengukuran level keamanan sebuah algoritma *block cipher* dapat dilakukan dengan 2 (dua) cara, yaitu melakukan pengujian pemetaan fungsi acak secara teoritis berdasarkan sifat matematis dan statistik, serta melakukan serangan berdasarkan karakteristik komponen, dan struktur dari algoritma *block cipher* tersebut. Serangan terhadap algoritma *block cipher* yang umum dilakukan adalah *Differential Attack* dan *Linear Attack*. Pada penelitian ini akan dilakukan analisis dengan menggunakan *differential attack* terhadap algoritma PRESENT. *Differential attack* merupakan serangan atau teknik kripanalisis yang termasuk ke dalam asumsi *chosen-plaintext attack*. Serangan ini akan diterapkan pada 5 *round*, 10 *round*, dan 15 *round* dan pada 1 *byte*, 2 *byte*, dan 3 *byte* aktif berdasarkan karakteristik sbox dan pbox algoritma PRESENT. Hasil pada penelitian ini akan menunjukkan bahwa *differential attack* pada algoritma PRESENT 5 *round* dan10 *round* lebih baik dibandingkan dengan menerapkan serangan praktis seperti *brute force attack*, sedangkan pada algoritma PRESENT 15 *round differential attack* akan tidak lebih efektif jika dibandingkan dengan *brute force attack*. Oleh karena itu dapat dikatakan bahwa algoritma PRESENT tahan terhadap *differential attack* untuk > 15 *round*.

Abstract

Measuring security level from a block cipher algorithm could be done by two methods, first method is conducting random testing of mapping functions base on mathematics and statistic properties, while the second method is attacking the algorithm base on its components and structure characteristics. Common attack that used to be done in block cipher algorithm are differential attack and linear attack. This paper would analyze PRESENT algoritm with differential attack. Differential attack is an attack or cryptanalysis technique which belong to the chosen-plaintext attack type of attacks. This attack would be applied into 5 round, 10 round, and 15 round, 1 byte, 2 byte, 3 byte active base on sbox and pbox characteristics of the PRESENT algorithm. The result of this paper would show that differential attack on 5 round and 10 round of PRESENT algorithm is better than applying practical attack like brute force attack, while differential attack on 15 round of PRESENT algorithm is not more effective than brute force attack. Therefore we could state that PRESENT algorithm would resistant to differential attack for more than 15 round.

Keywords: *Differential attack; block cipher; algoritma PRESENT.*

PENDAHULUAN

Sebuah algoritma *block cipher* yang baik seharusnya memiliki ketahanan terhadap segala serangan. Tingkat ketahanan sebuah algoritma *block cipher* harus ternilai secara ilmiah dengan menghitung kompleksitas serangan. Beberapa serangan terhadap algoritma *block cipher* diantaranya yaitu *Differential Attack*, *Linear Attack*, *Algebraic Attack*, *Boomerang*/*Rectangle Attack*, dll. Pada penelitian ini akan melakukan *differential attack* terhadap algoritma PRESENT. PRESENT merupakan algoritma standar untuk algoritma *lightweight block cipher* yang memiliki kriteria untuk penerapan pada *device* dengan sumber daya terbatas melalui ISO/IEC 29192-2.

Algoritma PRESENT menggunakan panjang blok 64 bit dengan panjang kunci 80 atau 128 bit. Jumlah *round* algoritma ini yaitu 31. PRESENT menggunakan struktur SPN sederhana yang terdiri dari *addRoundKey*, *SboxLayer*, dan *PboxLayer*.

Tabel 1. *Sbox* PRESENT

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Tabel 2 *Pbox* PRESENT

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
P(i)	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
P(i)	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
P(i)	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

AddRoundKey. Misal kunci *round* $K_i = [K_{63}^i,\ K_{62}^i, \dots ,\ K_1^i,\ K_0^i]$ untuk $1 \leq i \leq 32$ dan *state* $b_{63}, b_{62},\ \dots,\ b_1, b_0$ proses *key mixing* pada langkah *addRoundKey* terdiri atas operasi XOR berikut:

$b_j = b_j \oplus K_j^i$; untuk $0 \leq j \leq 63$

SboxLayer. *Sbox* yang digunakan pada PRESENT adalah *sbox* 4-bit ke 4-bit dengan notasi $S: \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^4$.
Untuk *sboxLayer* setiap *state* $b_{63}, b_{62},\ \dots,\ b_1, b_0$ dianggap sebagai 4-bit word sebanyak 16 yaitu $w_{15},\ \dots,\ w_0$ dimana $w_i = b_{4*i+3} \,||\, b_{4*i+2} \,||\, b_{4*i+1} || b_{4*i+0}$ untuk $0 \leq i \leq 15$.
Tabel substitusi *sbox* ditulis dalam heksadesimal seperti yang terlihat pada tabel 1.

PboxLayer. *PboxLayer* melakukan proses permutasi bit, dimana bit ke-i dari blok dipindah ke posisi bit pada $P(i)$.
Permutasi bit yang digunakan pada PRESENT menggunakan tabel permutasi seperti pada tabel 2.

METODE

Differential Attack

Differential attack dipublikasikan pertama kali oleh Eli Bilham dan Adi Shamir pada tahun 1990 untuk menyerang algoritma *block cipher* DES (*Data Encryption Standart*). Didalam perkembangannya, walaupun serangan tersebut pertama kali ditargetkan untuk menyerang algoritma *block cipher* DES, *differential attack* juga dapat diaplikasikan pada algoritma-algoritma kriptografi kunci simetrik lainnya, dimana *differential attack* merupakan salah satu serangan kriptanalisis yang paling kuat terhadap algoritma-algoritma kriptografi kunci simetrik.

Differential attack merupakan serangan atau teknik kripanalisis yang termasuk ke dalam asumsi *chosen-plaintext attack*. Ide dasar dalam teknik tersebut, yaitu pemilihan dua *plaintext* dengan adanya *difference* ΔP antara keduanya. Pada umumnya, *difference*nya diukur dengan menggunakan XOR ($\oplus$), setelah itu kedua *plaintext* tersebut dienkripsikan

untuk memberikan *output*, yaitu dua *ciphertext* yang memiliki *difference* ΔC diantara keduanya. Pasangan nilai $(\Delta P, \Delta C)$ tersebut disebut juga dengan karakteristik *differensial*. Tahap selanjutnya adalah bergantung pada algoritma kriptografi yang diserang dan analisis yang dilakukan oleh penyerang, dimana sifat nilai karakteristik tersebut dapat berguna untuk menemukan beberapa bit tertentu yang terdapat pada kunci.

Asumsi Serangan

Pada tulisan ini hanya akan membahas mengenai *differential attack* pada 5 *round*, 10 *round*, dan 15 *round* dengan menggunakan 1 *byte* aktif, 2 *byte* aktif, dan 3 *byte* aktif input *plaintext*. Penggunaan 15 *round* dari maksimal tidak terhingga *round* adalah karena masalah keterbatasan komputasi, dan harapannya hasil enkripsi dalam 15 *round* algoritma *block cipher* yang diserang telah lebih mangkus daripada hasil serangan praktis, yaitu *brute force attack*. Dimana dalam tulisan ini akan diasumsikan, bahwa hasil serangan 15 *round* yang tidak lebih mangkus daripada *brute force attack* adalah algoritma *block cipher* yang buruk. Sedangkan penggunaan serangan 3 *byte* aktif dari maksimal 8 *byte* aktif adalah karena kondisi karakteristik algoritma *block cipher* yang akan diuji dan juga masalah keterbatasan komputasi, dimana teknik dalam *differential attack* adalah menemukan *path* (jalur) berdasarkan pada karakteristik komponen substitusi dan struktur algoritma *block cipher*, dengan harapan hasil serangannya lebih mangkus dibandingkan dengan *brute force attack*. Dalam karakteristik *block cipher* yang akan diuji, input minimal 1 *byte* aktif akan menghasilkan setidaknya *output* minimal 1 *byte* aktif, sehingga apabila *input* yang digunakan adalah 8 *byte* aktif, maka minimal akan ada 1 *byte* aktif atau kurang lebih pengujian tersebut tidak akan lebih efektif dibandingkan dengan penggunaan 1 *byte* aktif saja, karena pada kondisi tertentu dan *round* ke-2 hasil dari input 8 *byte* aktif akan sama dengan hasil *output* dari 1 *byte* aktif.

Karakteristik *Sbox*

Karakteristik sebuah fungsi pemetaan acak (substitusi) pada sebuah algoritma *block cipher* dapat dicari dengan menggunakan pengujian XORTable pada *sbox* algoritma *block cipher* yang akan diserang. Pengujian XORTable merupakan teknik yang memanfaatkan operasi XOR, dimana operasi XOR memiliki kelemahan apabila penyerang menggunakan dua buah *plaintext* yang berbeda, maka penyerang dapat mengabaikan nilai *key* untuk menghasilkan sebuah karakteristik *differential*nya, dalam hal ini jika $P1 \oplus K = C1$ dan $P2 \oplus K = C2$ maka akan didapat :

$$C1 \oplus C2 = (P1 \oplus K) \oplus (P2 \oplus K)$$

$$=P1 \oplus K \oplus P2 \oplus K = P1 \oplus P2 \oplus K \oplus K = P1 \oplus P2$$

Sehingga dengan diasumsikan penyerang dapat memilih *plaintext* dan *ciphertext* (dalam mode serangan *chosen-plaintext attack*) maka penyerang dapat menggali karakteristik dari persamaan $P1 \oplus P2 = C1 \oplus C2$ dengan merangkum seluruh kemungkinan kemunculan pasangan $P1 \oplus P2$ dan $C1 \oplus C2$. Penyerang dapat memilih pasangan *plaintext* yang memiliki *difference* ΔP yang sedemikian sehingga memiliki peluang yang besar untuk menghasilkan *difference* output ΔC untuk kemudian dicari bit-bit kunci yang terafiliasi. Pada serangan *differential attack*, penyerang akan membentuk sebuah tabel yang berisi seluruh pasangan ΔP dan ΔC. Tabel ini sering disebut sebagai *Difference Distribution Table* (DDT) yang dalam pengujiannya juga disebut dengan XORTable. Dengan menjadikan ΔP sebagai baris dan ΔCsebagai kolom, maka tabel tersebut dapat diisi dengan:

$$XOR(\Delta P, \Delta C) = \#\{P \mid f(P) \oplus f(p \oplus \Delta P) = \Delta C\}$$

Salah satu teknik agar sebuah fungsi f atau algoritma *block cipher* tahan terhadap serangan *differential attack*, maka nilai entri pada XORTable tidak besar, idealnya bernilai (0) nol atau (2) dua dengan pengecualian pada entri (0,0) yang selalu bernilai 2^n. Hasil pengujian XORTable pada *sbox* algoritma PRESENT ditunjukan pada tabel 3.

Tabel 3 Hasil Pengujian XORTable pada *Sbox* Algoritma PRESENT

		OUTPUT															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
I	**0**	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N	**1**	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
P	**2**	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
U	**3**	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
T	**4**	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
	5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
	6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
	7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
	8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
	9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
	a	0	0	2	2	0	4`	0	0	2	0	2	0	0	2	2	0
	b	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
	c	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
	d	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
	e	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
	f	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

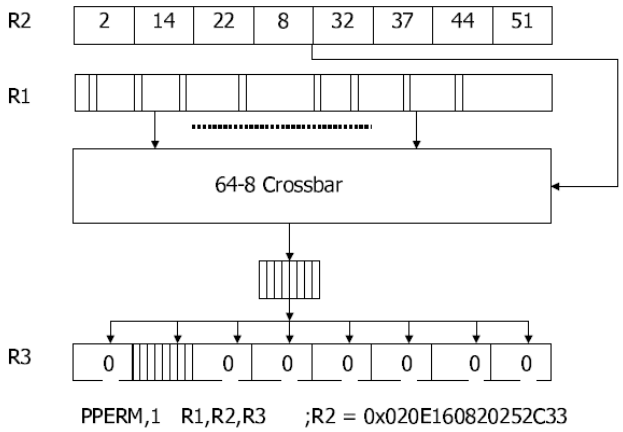
Tabel 4 Asumsi Serang *Differential Attack* pada Algoritma PRESENT

Input	1	2	3	4	5	6	7	8	9	a	B	c	d	e	f
Output	3	5	1	5	1	2	1	3	4	2	8	2	2	2	1
Probabilitas	4	4	2	4	2	2	4	2	4	2	4	2	4	2	4

Resume asumsi yang dapat digunakan dalam *differential attack* berdasarkan pada hasil pengujian XORTable pada pemeteaan fungsi acak (substitusi) algoritma PRESENT dapat dilihat pada tabel 4.

Karakteristik *Pbox*

Permutasi bit adalah bentuk lain dari operasi transposisi, yang memetakan 1 bit dari sumber ke tujuan, berdasarkan pada aturan/kontrol data tertentu. Selain itu permutasi bit juga dapat didefisnisikan sebagai pengurutan bit pada tujuan berdasarkan pemetaan bit dari sumber. Permutasi pada algoritma PRESENT didesain dengan menggunakan teknik permutasi PPERM, yaitu teknik permutasi yang memetakan k-bit (dari sumber) sesuai dengan posisi permutasinya (ke tujuan) berdasarkan pada konfigurasi kontrol bitnya. Parameter teknik permutasi PPERM ditunjukan pada gambar 1.



Gambar 1 Teknik Permutasi PPERM

Tabel 5 Resume Asumsi Serang *Differential Attack* pada *Pbox* Algoritma PRESENT

No.	Bit Pos	*Byte* Pos	Hasil	*Output Word*
1.	0_L	*Odd*	0	1
		Even	2	
	1_L	*Odd*	0	2
		Even	2	
	2_L	*Odd*	0	3
		Even	2	
	3_L	*Odd*	0	4
		Even	2	
2.	0_H	*Odd*	1	1
		Even	3	
	1_H	*Odd*	1	2
		Even	3	
	2_H	*Odd*	1	3
		Even	3	
	3_H	*Odd*	1	4
		Even	3	

Tabel 6 *Differential Attack* Algoritma PRESENT

No.	*Byte* Aktif	*Best Attack*	3 (Tiga) Contoh Nilai *Input*
Algoritma PRESENT (5 *Round*)			
1.	1 *Byte* Aktif	2^21	7700000000000000 7f00000000000000 9900000000000000
2.	2 *Byte* Aktif	2^20	0770000000000000 07f0000000000000 0990000000000000
3.	3 *Byte* Aktif	2^22	7700000000000707 770000000000070f 7700000000000f07
Algoritma PRESENT (10 *Round*)			
1.	1 *Byte* Aktif	2^48	7700000000000000 7f00000000000000 9900000000000000
2.	2 *Byte* Aktif	2^46	0700000000000700 0700000000000f00 0900000000000900
3.	3 *Byte* Aktif	2^50	7000000770000000 70000007f0000000 7000000f70000000
Algoritma PRESENT (15 *Round*)			
1.	1 *Byte* Aktif	2^74	1100000000000000 2200000000000000 2400000000000000
2.	2 *Byte* Aktif	2^72	0110000000000000 0220000000000000 0240000000000000
3.	3 *Byte* Aktif	2^76	7000000770000000 70000007f0000000 7000000f70000000

Teknik permutasi PPERM kurang lebih akan membutuhkan 64/8 *network crossbar*, karena untuk menghasilkan *output* PPERM membutuhkan 8 bit/*cycle*. 8 bit tersebut dapat berasal dari 64 bit *input* manapun, serta dapat dipetakan ke 8 bit *output* berbeda. Resume asumsi yang dapat digunakan dalam *differential attack* berdasarkan pada hasil pemetaan fungsi linear (permutasi) algoritma PRESENT ditunjukan pada tabel 5.

HASIL DAN PEMBAHASAN

Dengan menggunakan kedua karakteristik *sbox* dan *pbox* algoritma PRESENT, maka dapat dilakukan serangan pada algoritma tersebut pada 5 *round*, 10 *round*, dan 15 *round*. Hasil *differential attack* algoritma PRESENT dapat ditunjukan pada tabel 6.

Berdasarkan tabel 6 terlihat bahwa layer substitusi pada algoritma PRESENT memiliki *sbox* dengan karakteristik substitusi yang baik, sehingga kuat terhadap serangan *differential attack* untuk > 15 round, dalam hal ini serangan *differential* tidak lebih baik daripada serangan *brute force attack*. Begitu juga dengan layer permutasi pada algoritma PRESENT yang memiliki *pbox* dengan karakteristik permutasi yang baik, dimana layer permutasi tersebut dapat menyebarkan *output* dari fungsi pemetaan acak, sehingga dapat menyebarkan hasil *output* pada layer substitusi dengan baik.

SIMPULAN

Berdasarkan pada hasil pembahasan diatas dapat diambil beberapa kesimpulan, antara lain :

1. *Differential attack* terbaik pada 5 *round* algoritma PRESENT adalah 2^{20};
2. *Differential attack* terbaik pada 10 *round* algoritma PRESENT adalah 2^{44};
3. *Differential attack* terbaik pada 15 *round* algoritma PRESENT adalah 2^{70};
4. Algoritma PRESENT tahan terhadap *differential attack* untuk > 15 *round* karena tidak lebih baik daripada *brute force attack* (2^{64}).

DAFTAR PUSTAKA

Bogdanov, A., et al. (2007). *PRESENT: An Ultra-Lightweight Block Cipher*. CHES 2007, LNCS4727, pp.450- 466, Springer.

Eli, Biham and Shamir, Adi. (1990). *Differential Cryptanalysis of DES-like Cryptosystems*. Advances in Cryptology — CRYPTO '90. Springer-Verlag. 2–21.

LEE, R. B., et al. (2004). *Permutation Operations in Block Ciphers*. Diakses tanggal 19 Agustus 2015, pada http://palms.ee.princeton.edu/PALMSopen/ lee04permutation_book.pdf.

Menezes, Alfred J., Ooschot, Paul C. Van. & Vanstone, Scott A. (1997). *Handbook of Applied Cryptography*. Boca Raton : CRC press LLC.

Schneier, Bruce. (1996). *Applied Cryptography : Protocol, Algorithms and Source Code in C*. John Willey & Sons, Inc.

Sumarkidjo, dkk. (2007). *Jelajah Kriptologi*. Buku Tidak Diterbitkan. Jakarta. Lembaga Sandi Negara Republik Indonesia.