ALGORITMA *AUTHENTICATED ENCRYPTION PUBLIC KEYCRYPTOSYSTEM*BERBASIS*CARMICHAEL FUNCTION* (AECF)

Indra Setia Rahmat
Sekolah Tinggi Sandi negara
Jalan Raya Haji Usa, Desa Putat Nutug, Bogor, Bogor, 16330
Telp : (0251) 8541742/8541754, Fax : (0251) 8541720
E-mail : insertrahmat@gmail.com[1)]

Abstrak

Confidentiality dan authenticity data sering digunakan di dalam komputer moderen dan dalam teknologi komunikasi. Banyak apliasi dan protokol yang membutuhkan layanan confidentiality dan authenticity dalam keamanan, tetapi sampai saat ini dua layanan ini di desain secara terpisah sehingga tidak efisien. Authenticated encryption adalah suatu istilah yang digunakan untuk mengambarkan sistem enkripsi yang sekaligus menyediakan layanan confidentiality dan authenticity dalam komunikasi, Public key cryptosystems seperti RSA dan ElGamal hanya menyediakan layanan confidentiality. Dalam paper ini telah didesain algoritma authenticated encryption public key cryptosystems yang berbasis carmichael function (algoritma AECF) yang mendukung layanan confidentiality dan authenticity. Algoritma AECF mengkombinasi discrete logarithm problem dan factorization problem yang akan membuat cryptosystem lebih tahan terhadap beberapa serangan. Algoritma AECF menggunakan publik modulus kuadrat sehingga lebih efisien untuk memproses data yang besar, selain itu dengan publik modulus kuadrat lebih tahan degenerate keys.

Kata kunci: *Public key cryptosystems, authenticated encryption, carmichael function, algoritma AECF,degenerate keys.*

1. PENDAHULUAN

1.1 Latar Belakang

Dengan semakin pesatnya perkembangan Ilmu Pengetahuan dan Teknologi (IPTEK), maka semakin memudahkan setiap orang melakukanpertukaran informasi melalui berbagai media yang ada. Namun informasiyang dipertukarkan tidak terlepas dari kemungkinan disadap, dirusakataupun dirubah oleh pihak yang tidak bertanggung jawab ataupun yangtidak memiliki kewenangan terhadap informasi tersebut. Salah satu solusi dari permasalahan tersebut adalah dengan menerapkan kriptografi. Kriptografi adalah pembelajaran tentang teknik matematika yang memberikan layanan pengamanan berupa *confidentiality*, *data integrity*, *authenticity*[7]. Layanan *confidentiality* dan *authenticity* adalah layanan yang sering digunakan dalam pengamanan komunikasi [1]. Banyak aplikasi dan protokol komunikasi yang membutuhkan kedua bentuk layanan keamanan ini, namun sampai saat ini dua layanan ini di rancang secara terpisah [9], contoh penggunaan layanan *confidentiality* dan *authenticity*antara lain dalam pertukaran *session key* antar *node* dalam suatu jaringan, pertukaran *session key* dalam komunikasi rahasia antar dua pihak [9].Layanan *confidentiality* dan *authenticity* yang dirancang secaraterpisah atau *independen*kurang efisien untuk diterapkan [4], sebagai contoh algoritma RSA, AES, DES yang hanya menyediakan layanan *confidentiality*, sementara algoritma *digital signature*RSA atau *digital signature*ElGamal yang hanya menyediakan layanan *authenticity*, sehingga tidak efisien jika kedua algoritma ini di kombinasikan, karena akan terjadi dua proses yang saling independen. Oleh karena itudi perlukan sebuah desain satu algoritma yang sekaligus dapat menyediakan layanan *confidentiality*dan *authenticity*.

Dalam beberapa tahun ini telah dikembangkan algoritma baru yang menyediakan layanan *confidentiality* dan*authenticity* baik dalam algoritma simetrik maupun asimetrik yaitu algoritma *authenticated encryption* (AE). Algoritma *authenticated encryption* adalah suatu istilah yang digunakan untuk mengambarkan sistem enkripsi yang secara bersama melindungi *confidentiality* dan *authenticity* dalam komunikasi [9]. Namun saat ini algoritma simetrik *authenticated encryption* cenderung lebih berkembang dibanding algoritma asimetrik *authenticated encryption*. Padahal penggunaan algoritma asimetrik *authenticated encryption* sangat dibutuhkan terutama dalam pertukaran *session key* dalam komunikasi.

Saat ini algoritma asimetrik yang banyak digunakan dalam teknologi dan dapat digunakan dalam mengamankan komunikasi yang tidak aman adalah algoritma RSA dan algoritma ElGamal. Kedua algoritma ini digunakan sebagaistandar protokol *Virtual Private Network* (VPN), *Internet protocol security* IPSEC, *Pretty Good Privacy* (PGP), *Socket Secure Layer* (SSL) untuk mengamankan transmisi data pada jaringan publik dan untuk mengamankan komunikasi web dan email [5].

Salah satu permasalahan dalam algoritma RSA (RSA *problem*) adalah permasalahan pada pemfaktoran (*factorization problem*), jika diberikan n, maka sulit untuk mendapatkan nilai p dan q, dimana $n = p.q$ [6], sementara permasalahan dalam ElGamal adalah penyelesaian permasalahan logaritma diskrit (*Discrete Logarithm Problem*) diberikan nilai α dan α^x dalam finite field $\mathbb{F}_p$ maka sulit untuk mendapatkan x [7]. Jika *attacker* dapat menyelesaikan permasalahan *discrete logarithm problem* dan*factorization problem* maka akan mudah mengetahui pesan enkripsi.

Dalam paper ini telah di desain suatu algoritma asimatris *public key cryptosystem* bebasis *carmichael function* yang menyediakan layanan *confidentiality* dan *authenticity*, yang didesain berdasarkan kombinasi dari *Discrete Logarithm Problem* dan *factorization problem* sehingga diharapkan tahan terhadap beberapa serangan pada algoritma RSA dan algoritma ElGamal, selain itu algoritma AECF ini menggunakan nilai modulus kuadrat sehingga diharapkan lebih efisien untuk memproses data yang besar, selain itu dengan nilai modulus kuadrat dapat mencegah terjadinya *degenerate keys.* Jika dalam proses enkripsi terjadi *degenerate key* maka akan menyebabkan suatu pesan terenkripsi menghasilkan pesan yang sama dengna pesan awal.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah tersebut, maka rumusan masalah difokuskan pada:
1) Bagaimana proses pembangkitan pasangan kunci, proses enkripsi dan dekripsi algoritma AECF yang bebasis *carmichael function*?
2) Bagaimana analisis keamanan dan analisis serangan algoritma AECF ?

Analisis keamanan dan analisis serangan tidak dilakukan secara empiris hanya berdasarkan teoritis.

1.3 Tujuan

Tujuan penulisan ini adalah sebagai berikut :
1) Terwujudnya suatu algoritma asimetris yang dapat menyediakan layanan *confidentiality* dan*authenticity*yang berbasis *carmichael function.*
2) Menganalisis serangan *known k-parameter attack, man-in-the-middle attack* dan beberapa serangan yang berbasis *discrete logarithm proble*dan *factorization problem.*

2. LANDASAN TEORI

Berikut ini akan dijelaskan landasan teori tentang konsep teori bilangan, RSA*problem* dan *Discrete Logarithm Problem*, *degenerate keys.*

2.1 Theorema

Theorema *Carmichael function*
Dua buah bilangan primer p dan $q$maka berlaku persamaan $m^{\lambda(n)} = 1\ mod\ N,\ \lambda(n) = lcm\left((p-1)(q-1)\right), \gcd(m, N) = 1$ untuk semua $m \in N$ [12].
Theorema Euler
Jika $\boldsymbol{n}$ adalah bilangan positif dan gcd $(\boldsymbol{a}, \boldsymbol{n}) = \boldsymbol{1}$, maka $\boldsymbol{a^{\emptyset(n)} \equiv 1\ mod\ p}$ [6].
Theorema Fermat
Jika p adalah bilangan prima dan a integer positif yang tidak dapat dibagi oleh p, maka $a^{p-1} \equiv 1\ mod\ p$ [6].

2.2 RSA *problem*

Definisi : jika diberikan integer positif $\boldsymbol{n}$yang merupakan hasil perkalian dua bilangan prima p dan q, sebuah integer positif e sedemikian sehingga $\gcd\left(e, (p-1)(q-1)\right) = 1$ dan integer c, untuk mendapatkan integer m sedemikian sehingga $m^e \equiv c\ \boldsymbol{mod}\ n$ [7].

2.3*Discrete Logarithm Problem* (DLP)

Definisi : jika diberikan bilangan prima p, sebuah generator α di $\mathbb{Z}_p^*$ dan elemen $\beta \in \mathbb{Z}_p^*$,untuk mendapatkan integer $x, 0 \leq x \leq p-2$, sedemikian sehingga $\boldsymbol{a^x \equiv \beta\ mod\ p}$ [7].

2.4*Degenerate Keys*[2]

Definisi : algoritma RSA (m, e) dikatakan terjadi d*egenerate keys* jika dan hanya jika$m^e mod\ n = m$ untuk scemua $m < n$.
Contoh

1. $p = 5, q = 13$
2. Hitung $n = 5.13 = 65$
3. Hitung $\emptyset(n) = 4.12 = 48$
4. Pilih bilangan bulat (integer) e, $1 < e\ < \psi$, dimana $\gcd(e, 48) = 1,\ e = 13$
5. Diketahi pesan$m$ dalam integer adalah 4, 5, 6, 64.
   $C = 4^{13}\ mod\ 65 = 4$
   $C = 5^{13}\ mod\ 65 = 5$
   $C = 6^{13}\ mod\ 65 = 6$
   $C = 64^{13}\ mod\ 65 = 64$

AlgoritmaRSA terjadi *degenerate* jika dan hanya jika $lcm\ ((p-1),(q-1))|\ e-1$ dimana $n = p.q$. Dari contoh diatas didapatkan*degenerate key* yang lain yaitu $e = 25$ dan $e = 37$ karena $lcm\ (4{,}12) = 12$ dimana 12 | (13-1) untuk $n = 65$, sehingga untuk $e = 25, 12 \mid 24$ dan $e = 37, 12 \mid 36$.
Untuk mengetahui jumlah *degenerate keys* dalam algoritma RSA menggunakan persamaan
$N = \frac{\emptyset(n)}{lcm(p-1,q-1)} - 1$, dengan *N* adalah jumlah *degenerate keys*, $\emptyset(n) = (p-1)(q-1)$.
Degenerate key menyebabkan suatu pesan yang terenkripsi menghasilkan pesan yang sama dengna pesan awal.

3. METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode kajian kepustakaan dan metode eksperimen. Penelitian diawali dengan studi literatur yang diambil dari buku, buku elektronik maupun sumber-sumber yang berhubungan dengan penelitian dilanjutkan dengan tahap desain algoritma, analisis dan kesimpulan.

3.2 Tahapan Penelitian

Tahapan dalam penelitian ini adalah:
1) Pengumpulan Data.
Studi literatur tentang theorema *carmichael function*, RSA *problem, discrete logarithm problem (DLP), degenerate keys,* dan *authentication encryption*
2) Membuat desain algoritma AECF.

a. Membuat desain algoritma AECF berdasarkan theorema *carmichael function,* RSA *problem, discrete logarithm problem (DLP)*dan *degenerate keys.*

Berikut tahapan desan algoritma AECF:

1. Berdasarkan theorema *carmichael function*$m^{\lambda(n)} = 1\ mod\ N$, $\lambda(n)\ = lcm\ \big((p-1)(q-1)\big), \gcd(m, N) = 1$, apabila niali $\lambda(n)$ dilakukan operasi perkalian dengan N, maka akan berlaku persamaan $m^{N\lambda(n)} = 1\ mod\ N^2$ atau dapat dituliskan $m^{\psi} = 1\ mod\ N^2$ dimana $\psi = N.\lambda(n)$.Nilai modulus N^2akan mencegah terjadinya *degenerate keys,* karena semakin besar nilai modulus maka akan semakin kecil kemungkinan terjadinya *degenerate keys.*
2. Dalam proses *confidentiality*didasarkan pada persamaan $m^{\psi} = 1\ mod\ N^2$, sesuai prinsip RSA *problem*dengan memilih bilangan bulat e, $1 < e\ < \psi$, dimana $gcd\ (e, \psi) = 1$ dan menghitung d, $1 < d < \psi$,dimana $e.d \equiv 1\ (mod\ \psi)$ didapatkan pasangan nilai e dan d yang saling invers, karena saling invers maka dapat digunakan dalam proses enkripsi dan dekripsi.
3. Dalam proses *authenticity*(*entitas*) masing – masing pihak memilih nilai lB dan lA dimana lB dan $lA \in N^2$ dan membangkitkan nilai $\beta_A$dan $\beta_B$dengan menghitung $\beta_A = \alpha^{lA}\ mod\ N^2$dan $\beta_B = \alpha^{lB}\ mod\ N^2$ dimana nilaiα adalah nilai publik. Nilai $\beta_A$dan β_B merupakan *public key*, lB dan lAmerupakan*private key*. *Authenticity (entitas)* dihasilkan dari enkripsi dengan menggunakan *private key*sehingga menjamin keaslian identitas pengirim.Nilai ${\beta_A}^{lB}$merupakan invers dari nilai $({\beta_A}^{lB})^{-1}$ sehingga proses enkripsi dan dekripsi tetap dapat berjalan.
4. Proses *confidentiality*dan proses *authenticity*(*entitas*) digabungkan menghasilkan algoritma AECF.

b. Melakukan pembuktian matematis untuk membuktikan bahwa desain algoritma AECF dapat melakukan proses enkripsi dan dekripsi dengan benar.
c. Melakukan implementasi menggunakan bahasa pemograman C++ untuk membuktikan sistem enkripsi dan dekripsi bekerja.

3) Melakukan analisis
Analisis algoritma AECF meliputi analisis efisiensi, analisis keamanan dan analisis serangan.
3) Menarik kesimpulan menegenai algoritma AECF.

4. ALGORITMA AECF

Berikut ini desain algoritma *authenticated encryption public key cryptosystem* berbasis *carmichael function* (AECF).

4.1 Algoritma AECF

Key Generation
Misal Bob akan berkomunikasi dengan Alice, maka Bob dan Alice membangkitkan pasangan kunci, diasumsikan*public*α dan k, *public key* Alice = $\{N_A^2, eA, \beta_A\}$, *private key Alice*= $\{dA, lA\}$ dan *public key*Bob = $\{N_B^2, eB, \beta_B\}$, *private key*Bob= $\{dB, lB\}$.

1) Memilih bilangan prima p dan q
2) Menghitung $N_A^2 = (pq)^2$
3) Menghitung$\lambda(n) = lcm\ ((p-1)(q-1))$
4) Menghitung$\psi = N_A\lambda(n)$
5) Memilih bilangan acak $k, gcd\ (k, N_A^2) = 1$
6) Memilih bilangan bulat e, $1 < e < \psi$, dimana $gcd\ (e, \psi) = 1$
7) MenghitungdA, $1 < dA < \psi$,dimana $eA.dA \equiv 1\ (mod\ \psi)$
8) Memilih $lA \in N_A^2$, dan menghitung$\beta_A = \alpha^{lA}\ mod\ N_A^2$
9) *Public key* = $\{N_A^2, eA, \beta_A\}$, , *private key* = $\{dA\}$

Encryption
Bob akan mengenkripsi *plaintextm* menggunakan *public key*Alice = $\{N_A^2, eA, \beta_A\}$
1) Menghitung$r = k^{eA}\ mod\ N_A^2$
2) Menghitung$s = m.k.{\beta_A}^{lB} mod\ N_A^2$
3) *Ciphertextc* (r, s)

Decryption
Alice dapat mendekripsi *ciphertextc* menggunakan *private key Alice*= $\{dA, lA\}$
1) Menghitung$m = s.(r^{dA})^{-1}.({\beta_B}^{lA})^{-1} mod\ N_A^2$

4.2 Pembuktian matematis

Berdasarkan teorema *Carmichael function*

$m^{\lambda(n)} = 1\ mod\ N, \lambda(n) = lcm\ \big((p-1)(q-1)\big), \gcd(m, N) = 1.$
$m^{N\lambda(n)} = 1\ mod\ N^2$
$m^{\psi} = 1\ mod\ N^2$
$s.(r^{dA})^{-1}.({\beta_B}^{lA})^{-1} = m.k.((k^{eA})^{dA})^{-1}.{\beta_A}^{lB}.({\beta_B}^{lA})^{-1} = m.k.(k^{1+x\psi})^{-1}.1.1 = m.k.k^{-1}.1.1.1 = m$

4.3 Contoh

Key Generation
Misal Bob akan berkomunikasi dengan Alice, maka Bob dan Alice membangkitkan pasangan kunci, diasumsikan *public*$\alpha = 23$ dan $k = 50$, *Public key*Alice = $\{20449,181,6062\}$, *private key*Alice= $\{5641,17\}$, *public key* Bob = $\{48841,271,14026\}$,*private key* Bob= $\{5167,27\}$.

1) Bilangan prima $p = 11$ dan $q = 13$
2) Menghitung $N_A^2 = (pq)^2 = (11.13)^2 = 143^2 = 20449$
3) Menghitung $\lambda(n) = lcm\ \big((p-1)(q-1)\big) = lcm\ ((11-1),(13-1)) = 60$
4) Menghitung$\psi = N_A\lambda(n) = 143.60 = 8580$
5) Bilangan $k = 50$
6) Bilangan $eA = 181$
7) Bilangan $dA = 181^{-1} mod\ 8580 = 5641$
8) Memilih $lA = 17$Menghitung$\beta_A = \alpha^{lA}\ mod\ N_A^2 = 23^{17} mod\ 20449 = 6062$
9) *Public key*Alice = $\{20449,181,6062\}$, *private key*Alice= $\{5641,17\}$

Encryption
Bob akan mengenkripsi *plaintextm* $= 128$ menggunakan *public key*Alice = $\{20449,181,6062\}$,
1) Menghitung $r = k^{eA}\ mod\ N_A^2 = 50^{181}\ mod\ 20449 = 5198$

2) Menghitung$s = m.k.{\beta_A}^{lB} mod\ N_A^2 = 128.50.6062^{27} mod\ 20449 = 10162$
3) *Ciphertextc* $(5198, 10162)$

Decryption
Alice dapat mendekripsi *ciphertextc* menggunakan *private key Alice*= $\{5641\}$
1) Menghitung$m = 15211.(5198^{5641})^{-1}.(14026^{17})^{-1} mod\ 20449 = 15211.409.12167\ mod\ 20449 = 128$

5. PEMBAHASAN DAN ANALISIS

Berikut akan dijelaskan analisis algoritma AECF dari segi efisiensi, layanan keamana dan serangan.

5.1 analisis efisiensi

Sebuah algoritma tidak hanya harus aman, tetapi juga harus efisiens, algoritma AECF menggunakan nilai modulus kuadrat (N^2)sehingga diharapkan lebih efisien untuk enkripsi data besar, namun algoritma AECF mengunakan dua buah *private key*sehingga kurang efisien jika dibanding algoritma RSA.Selain itu dengan menggunakan nilai modulus kuadrat akan mencegah terjadinya *degenerate keys,* karena semakin besar nilai modulus maka akan semakin kecil kemungkinan terjadinya *degenerate keys.*

5.2 layanan keamanan

Algoritma AECF menyediakan dua layanan yaitu *confidentiality dan authenticity(entitas).* Layanan *authenticity (entitas)* dihasilkan dari enkripsi dengan menggunakan *private key* sehingga menjamin keaslian identitas pengirim, selain itu enkripsi dengan menggunakan *private key* akan membuat algoritma AECF lebiih tahan terhadap serangan *known k-parameter attack*dan *man-in-the-middle attack.*

5.3 analisis serangan

5.3.1 *Known k-parameter attack*

Algoritma AECF lebih tahan terhadap serangan *known k-parameter attack* karena untuk melakukan enkripsi pesan tidak hanya menggunakan parameter k, sehingga apabila nilai k diketahui maka tetap sulit untuk mendapatkan m, penyerang harus mengetahui *private key* d.

$$s = m.k.\beta^l$$

5.3.2 *Man-In-the-middle attack*

Salah satu cara untuk mencegah terjadinya *man-in-the-middle attack* adalah dengan adanya *authenticity (entitas),* Algoritma AECF lebih tahan terhadap *man-in-the-middle attack*karena terdapat layanan *authenticity (entitas).*

5.3.3 Serangan logaritma diskrit dan exponen publik dan privat

Algoritma AECF mengkombinasi *discrete logarithm problem* dan*factorization problem* sehingga apabila *attacker* dapat menyelesaikan *discrete logarithm problem* dengan menggunakan serangan seperti *baby-step giant-step, silver-pohlig hellman, index calculus,* atau *xedni calculus attacker* tidak langsung bisa mendapatkan pesan karena pesan terenkripsi menggunakan kombinasi *discrete logarithm problem* dan*factorization problem,* sehingga *attacker* juga harus menyelesaikan permasalahan *factorization problem* dengan melakukan serangan seperti *eth root attack, common modulus attack, fixed-point attack, atau diophantine attack.*

6. SIMPULAN DAN SARAN

6.1 Simpulan

Dari hasil pembuatan desain algoritma asimetris *authenticated encryptionpublick key cryptosystem* berbasis *carmichael function*(algoritma AECF) yang telah dilakukan dapat disimpulkan sebagai berikut.

1. Algoritma AECF menyediakan layanan *confidentiality dan authenticity* sehingga lebih efisien untuk diterapkan dalam pengamanan informasi terutama untuk pertukaran *session key*.
2. Algoritma AECFmengkombinasi *discrete logarithm problem* dan *factorization problem*sehingga lebih tahan terhadap beberapa serangan pada algoritma yang berbasis *discrete logarithm problem* dan *factorization problem*, selain itu juga lebih tahan terhadap serangan *known k-parameter attack* dan *man-in-the-middle attack*.
3. Algoritma AECF menggunakan nilai modulus kuadrat sehingga lebih efisien untuk memproses data yang besar, selain itu dengan nilai modulus kuadrat mencegah terjadinya *degenerate keys, degenerate key* menyebabkan suatu pesan terenkripsi menghasilkan pesan yang sama dengna pesan awal.

6.2 Saran

Dalam pembuatan desain algoritma AECF ini didasarkan dari berbagai theorema antara lain *carmichael function,* RSA *problem, discrete logarithm problem (DLP), degenerate keys,* dan *authentication encryption* serta dasar serangan seperti *known k-parameter attack*dan *man-In-the-middle attack.* Meskipun secara matematis dan implementasi proses enkripsi dan dekripsi dapat dibuktikan berjalan namun kedepan perlu di lakukan penerapan dalam pengamanan informasi baik dalam aplikasi maupun protokol komunikasi sehingga dapat dianalisis lebih lanjut terkait analisis keamanan, efisiensi, dan serangan serta pengaruhnya terhadap terjadinya degenerate keys.

7. DAFTAR RUJUKAN

[1] Black, J., 2004. *Authenticated Encryption*. Department of Computer Science, Colorado.USA.

[2] Bergmann, Seth D; 2001. *Degenerate Keys for RSA Encryption*; Rowan University.

[3] Boneh, D., 2001. *Why Textbook ElGamal and RSA Encryption Are Insecure*. Stanford University, Computer Science Department Stanford, CA 94305, USA.

[4] Fitzgerald, Shawn., 2013. *An Introduction To Authenticated Encryption*. iSEC Partners, Inc. San Francisco.

[5] Jakob, M., 2012. *Authenticated And Secure El-Gamal Cryptosystem Over Elliptic Curves.*Department of Computer Information System.Amman Arab University.

[6] Kaliski, Burt; 1990.*The Mathematics of the RSA Public-Key Cryptosystem*; RSA Laboratories.

[7] Menezes, Alfred J. Paul C. van Oorschot, Scott A. Vanstone., 1997. *Handbook of Applied Cryptography*. CRC Press LLC: Boca Raton.

[8] Paillier, P., 1999. *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes*. EUROCRYPT; Springer.

[9] Pieprzyk., 2003.*Parallel Authentication and Public-Key Encryption.* The Eighth Australasian Conference on Information Security and Privacy (ACISP '03), Springer-Verlag, LNCS 2727, pages 383-401.

[10] Stallings, William., 2011. *Cryptography and Network Security, Principles and Practice*, *Fifth edition*. Pearson Education, Inc.

[11] Stinson, Douglas R., 2006. *Cryptography: Theory and Practice.* 3rd Edition. CRC Press. Florida

[12] Yan, Song Y., 2008. *Cryptanalytic Attacks on RSA.* Springer Science+Business Media, LLC.

[13] http://math-it.org/Mathematik/Zahlentheorie/Carmichael.html [Accessed 21 Juni 2015].