Perangkat Lunak Bantu Pembelajaran *Identity-Based Encryption* (IBE)

Oleh:
Yulius Zamili[1], Jeremia Siregar[2], Ruth Meivera Siburian[3]

Prodi Teknik Informatika, Fakultas Teknologi Industri
Institut Sains Dan Teknologi TD Pardede, Jl. DR. TD. Pardede No.8 Medan 20153

E-Mail:
zamilysharing@gmail.com[1], jeremiasiregar@istp.ac.id[2], v_manut@yahoo.com [3]

ABSTRAK

Identity-Based Encryption (IBE) adalah teknik enkripsi pengamanan data dengan menggunakan kunci asimetris yang mempunyai keistimewaan, yaitu public-key yang digunakan dapat berupa sembarang string sehingga data dapat diamankan tanpa perlu menggunakan sertifikat. Public-key pada Identity-Based Encryption ini dapat berupa alamat email, nomor telepon, ataupun suatu kalimat yang menunjukkan identitas dari penerima. Perangkat lunak ini menjelaskan proses dari masing-masing tahapan yang ada dalam metode kriptografi IBE ini. Perangkat lunak ini juga dilengkapi dengan algoritma-algoritma pendukung yang akan digunakan dalam proses perhitungan tahap-tahap kriptografi IBE. Perangkat lunak pembelajaran ini, diharapkan akan menjadi referensi dan studi awal bagi pembaca khususnya mahasiswa yang mempelajari mata kuliah kriptografi untuk mempelajari lebih lanjut mengenai kriptografi IBE.

Kata Kunci: Public Key, IBE, Kriptografi

ABSTRACT

Identity-Based Encryption (IBE) is a data security encryption technique that utilizes asymmetric keys. The public key can be any string, allowing data to be secured without the need for a certificate. The public key in Identity-Based Encryption can be an email address, a telephone number, or a sentence identifying the recipient. This software explains each step in the IBE cryptography method. It also includes supporting algorithms used in the calculation process for each step in IBE cryptography. This learning software is expected to serve as a reference and initial study for readers, especially students studying cryptography, to learn more about IBE cryptography.

Keyword : Public Key, IBE, Kriptografi

1. PENDAHULUAN

Pada dasarnya, enkripsi digunakan untuk melindungi data agar hanya orang tertentu (seperti Bob@yahoo.com) atau sebuah mesin yang hanya dapat mengakses data tersebut, seperti www.yahoo.com. Sampai saat ini, enkripsi masih menggunakan kunci acak yang panjang yang dipetakan untuk identitas tertentu dengan menggunakan dokumen yang ditandatangani secara digital, juga dikenal sebagai sertifikat. Pengguna selalu bertanya tentang masalah sertifikat, yang menyebabkan kesulitan mendapatkan kunci pribadi yang baru.

Identity-Based Encryption (IBE) menawarkan solusi baru untuk masalah enkripsi konvensional.

IBE memungkinkan penggunaan string apa pun sebagai kunci publik, sehingga data dapat disimpan tanpa perlu menggunakan sertifikat. Pengamanan dilakukan oleh key server, yang bertanggung jawab atas pemetaan identitas ke kunci dekripsi. Dalam dunia kriptografi, desain sistem IBE telah menjadi masalah terbuka. IBE, juga dikenal sebagai Enkripsi Berbasis Identitas, adalah metode enkripsi dengan menggunakan kunci asimetris yang memiliki keunggulan, yaitu kunci publik dapat digunakan dalam bentuk string apa pun. Kunci publik biasanya rumit dan sulit diingat untuk digunakan dalam enkripsi. Identitas Berbasis Enkripsi menggunakan kunci publik yang lebih "ramah pengguna". Kunci publik ini dapat berupa kalimat, nomor telepon, atau alamat email.

Kelebihan lain dari metode enkripsi ini adalah bahwa tidak perlu menentukan pasangan kunci sebelum melakukan enkripsi. Dengan Identity-Based Encryption, seseorang dapat mengirimkan email yang telah dienkripsi dengan kunci publik bahkan jika penerima email tidak pernah mendengar kunci pribadi. Setelah email diterima, penerima akan menghubungi private-key Generator, yang kemudian akan melakukan autentikasi dan memberikan private-key untuk membaca email tersebut.

Algoritma IBE adalah sebuah tipe algoritma kriptografi public key dimana public key tersebut dikalkulasikan secara langsung dari sebuah identitas user bukan dihasilkan secara acak atau random. Ini memerlukan sebuah set langkah berbeda dari enkripsi dan deskripsi dan akan digunakan dengan public key lainnya. Skema enkripsi berbasis identitas yang paling efisien saat ini didasarkan pada bilinear pairing pada kurva elips, seperti pemasangan Weil atau Tate. Weil Pairing adalah salah satu metode pemetaan bilinear antar grup. Hingga beberapa waktu lalu, Weil pairing telah sering digunakan untuk menyerang sistem kurva elips. Joux baru-baru ini menunjukkan bahwa Weil Pairing dapat digunakan untuk “kebaikan” dengan cara menggunakannya untuk sebuah protokol bagi penukaran kunci satu putaran tiga pihak Diffie-Hellman. Sakai et al menggunakannya untuk penukaran kunci dan Verheul menggunakannya untuk mengkonstruksi sebuah skema enkripsi ElGamal dimana masing-masing kunci publik memiliki dua kunci pribadi yang berkorespondensi.

Keunggulan utama IBE adalah kesederhanaannya. IBE memudahkan mekanisme pengamanan komunikasi, di mana pesan dapat dienkripsi dan diautentikasi secara langsung, dengan menggunakan identifikasi yang sudah banyak dikenal, seperti alamat email, sebagai kunci publik. IBE dapat digunakan untuk membuat sistem keamanan yang lebih kecil, fleksibel, dan skala besar. Kelemahan sistem IBE adalah bahwa kunci privat harus dikirimkan dari PKG ke user. Oleh karena itu, jalur atau kanal yang aman diperlukan untuk menjamin keaslian dan kerahasiaan kunci tersebut.

Dari penjelasan di atas, maka penulis bermaksud untuk merancang perangkat lunak pembelajaran IBE dengan judul Perancangan Perangkat Lunak Pembelajaran IBE.

2. TINJAUAN PUSTAKA

Konsep IBE ditemukan pada tahun 1984 oleh Adi Shamir dalam rangka mengatasi masalah autentikasi kunci public. Idenya adalah untuk menghindari kebutuhan autentukasi dengan cara kunci publik yang digunakan berhubungan langsung dengan identitas user.

Teknik IBE oleh Boneh dan Franklin adalah yang pertama yang efektif dan aman. Untuk mengenkripsi pesan, pengirim menggunakan peta bilinear untuk menggabungkan identitas penerima, parameter sistem dari PKG, dan kunci master menjadi kunci enkripsi. Selain itu, penerima pesan dapat menggunakan peta bilinear untuk menggabungkan kunci privat penerima dan parameter publik yang dikirimkan bersama ciphertext.

3. METODE PENELITIAN

Teknik IBE oleh Boneh dan Franklin adalah yang pertama yang efektif dan aman. Bilinear map digunakan oleh pengirim untuk mengenkripsi pesan dengan menggabungkan identitas penerima, parameter sistem PKG, dan kunci master menjadi kunci enkripsi. Dengan menggunakan map ini, penerima pesan dapat menghasilkan kunci untuk dekripsi.

Untuk menggabungkan parameter publik yang dikirimkan bersama ciphertext dengan kunci penerima privat. Secara keseluruhan, metode ini dapat digambarkan sebagai berikut:

1. Setup

PKG mengambil dua titik pada kurva elips, yaitu titik P dan master key s, untuk menginisialisasi IBE.

Melalui penggunaan generator angka acak P dan s • P, parameter publik, kemudian dibagikan ke semua user, biasanya melalui sertifikat server. Selain itu, master key dapat dibagi secara rahasia, sehingga tidak ada server yang dapat mengganggu sistem.

2. Extract

Bob tidak memiliki kunci k untuk mendekripsi pesan Alice ketika dia menerimanya. Oleh karena itu, dia perlu melakukan autentikasi ke PKG. Setelah dia autentikasi, server menghitung s • IDBob dan memberikannya kepada Bob. Nilai ini merupakan kunci privat Bob.

3. Encrypt

Untuk mengirimkan pesan kepada Bob, Alice memetakan identitas Bob, misalnya bob@yahoo.com, ke suatu titik pada kurva elips IDBob. Kemudian dia memilih angka acak r dan menghitung kunci k, yang ditulis dalam persamaan berikut:

k = Pair (r • IDBob, s • P).

Setelah mendapatkan kunci, Alice mengenkripsi pesan dengan k, Ek[Pesan], dan juga mengirimkan hasil perkalian r • P.

4. Decrypt

Kunci k dapat diperoleh Bob setelah menerima pesan dan hasil perkalian r • P dengan menghitung:

k = Pair (s • IDBob, r • P).

Karena sifat bilinear map, kunci k di atas sama dengan kunci yang digunakan Alice untuk mengenkripsi pesan, yaitu:

k = Pair (r • IDBob, s • P)

Bob dapat mendekripsi pesan yang dia terima dengan menggunakan kunci k. Tidak ada orang lain yang dapat menghitung kunci privat Bob, yaitu s • IDBob.

3.1 Algoritma IBE

Secara umum, teknik IBE terdiri dari empat algoritma, yaitu:

• Konfigurasi: menentukan parameter sistem dan tombol master dengan mengambil beberapa parameter kemanan dari input.

Algoritma ini dijalankan oleh PKG. Parameter sistem termasuk deskripsi ruang plaintext dan ciphertext. Namun, master key hanya dapat diketahui oleh PKG.

• Extract, yaitu menghasilkan identitas kunci privat dID yang sesuai dengan identitas kunci publik (string yang digunakan) dari

Parameter sistem, master key, dan identitas ID adalah {0,1}. Selain itu, algoritma ini digunakan oleh PKG saat pengguna meminta kunci privatnya untuk mendekripsi pesan dengan memberikan string yang digunakan untuk menghasilkan kunci publik. Dalam situasi ini, pengguna harus membuktikan kepada PKG bahwa dia benar-benar pemilik string atau identitas tersebut.

• Enkripsi adalah algoritma yang digunakan oleh pengguna untuk mengenkripsi pesan M untuk pengguna yang dimaksud dengan menggunakan kunci publik, dan parameter sistem menghasilkan ciphertext.

• Decrypt, yang menggunakan kunci privat dID dan parameter sistem untuk mendeskripsi ciphertext C, menghasilkan plaintext. Algoritma ini juga digunakan oleh pengguna.

4. HASIL dan PEMBAHAS

ENKRIPSI MULAI

==> XOR PLAINTEXT DENGAN H2(Qid, ppub_3user)

V(0) = Plaintext(0) XOR H2(0)

= 49 XOR 31

= 78

V(1) = Plaintext(1) XOR H2(1)

= 53 XOR 36

= 65

V(2) = Plaintext(2) XOR H2(2)

= 54 XOR 34

= 60

V(3) = Plaintext(3) XOR H2(3)

= 50 XOR 34

= 64

V(4) = Plaintext(4) XOR H2(4)

= 00 XOR 30

= 30

V(5) = Plaintext(5) XOR H2(5)

= 00 XOR 33

= 33

V(6) = Plaintext(6) XOR H2(6)

= 00 XOR 38

= 38

V(7) = Plaintext(7) XOR H2(7)

= 00 XOR 31

= 31

V(8) = Plaintext(8) XOR H2(8)

= 00 XOR 31

= 31

V(9) = Plaintext(9) XOR H2(9)

= 00 XOR 35

= 35

V(10) = Plaintext(10) XOR H2(10)

= 00 XOR 31

= 31

V(11) = Plaintext(11) XOR H2(11)

= 00 XOR 36

= 36

V(12) = Plaintext(12) XOR H2(12)

= 00 XOR 32

= 32

V(13) = Plaintext(13) XOR H2(13)

= 00 XOR 35

= 35

V(14) = Plaintext(14) XOR H2(14)

= 00 XOR 37

= 37

V(15) = Plaintext(15) XOR H2(15)

= 00 XOR 34

= 34

V(16) = Plaintext(16) XOR H2(16)

= 00 XOR 32

= 32

V(17) = Plaintext(17) XOR H2(17)

= 00 XOR 31

= 31

V(18) = Plaintext(18) XOR H2(18)

= 00 XOR 38

= 38

V(19) = Plaintext(19) XOR H2(19)

= 00 XOR 37

= 37

V(20) = Plaintext(20) XOR H2(20)

= 00 XOR 35

= 35

V(21) = Plaintext(21) XOR H2(21)

= 00 XOR 30

= 30

V(22) = Plaintext(22) XOR H2(22)

= 00 XOR 30

= 30

V(23) = Plaintext(23) XOR H2(23)

= 00 XOR 30

= 30

V(24) = Plaintext(24) XOR H2(24)

= 00 XOR 30

= 30

Karena H2 lebih pendek dari Plaintext, maka H2 diulang dari awal

V(25) = Plaintext(25) XOR H2(0)

= 00 XOR 31

= 31

V(26) = Plaintext(26) XOR H2(1)

= 00 XOR 36

= 36

V(27) = Plaintext(27) XOR H2(2)

= 00 XOR 34

= 34

V(28) = Plaintext(28) XOR H2(3)

= 00 XOR 34

= 34

V(29) = Plaintext(29) XOR H2(4)

= 00 XOR 30

= 30

V(30) = Plaintext(30) XOR H2(5)

= 00 XOR 33

= 33

V(31) = Plaintext(31) XOR H2(6)

= 00 XOR 38

= 38

V(32) = Plaintext(32) XOR H2(7)

= 00 XOR 31

= 31

V(33) = Plaintext(33) XOR H2(8)

= 00 XOR 31

= 31

V(34) = Plaintext(34) XOR H2(9)

= 00 XOR 35

= 35

V(35) = Plaintext(35) XOR H2(10)

= 00 XOR 31

= 31

V(36) = Plaintext(36) XOR H2(11)

= 00 XOR 36

= 36

V(37) = Plaintext(37) XOR H2(12)

= 00 XOR 32

= 32

V(38) = Plaintext(38) XOR H2(13)

= 00 XOR 35

= 35

V(39) = Plaintext(39) XOR H2(14)

= 00 XOR 37

= 37

V(40) = Plaintext(40) XOR H2(15)

= 00 XOR 34

= 34

V(41) = Plaintext(41) XOR H2(16)

= 00 XOR 32

= 32

V(42) = Plaintext(42) XOR H2(17)

= 00 XOR 31

= 31

V(43) = Plaintext(43) XOR H2(18)

= 00 XOR 38

= 38

V(44) = Plaintext(44) XOR H2(19)

= 00 XOR 37

= 37

V(45) = Plaintext(45) XOR H2(20)

= 00 XOR 35

= 35

V(46) = Plaintext(46) XOR H2(21)

= 00 XOR 30

= 30

V(47) = Plaintext(47) XOR H2(22)

= 00 XOR 30

DEKRIPSI MULAI

==> XOR V DENGAN H2(Did, U)

Plaintext(0) = V(0) XOR H2(0)

= 78 XOR 32

= 49

Plaintext(1) = V(1) XOR H2(1)

= 65 XOR 33

= 53

Plaintext(2) = V(2) XOR H2(2)

= 60 XOR 36

= 54

Plaintext(3) = V(3) XOR H2(3)

= 64 XOR 33

= 50

Plaintext(4) = V(4) XOR H2(4)

= 30 XOR 33

= 00

Plaintext(5) = V(5) XOR H2(5)

= 33 XOR 30

= 00

Plaintext(6) = V(6) XOR H2(6)

= 38 XOR 34

= 00

Plaintext(7) = V(7) XOR H2(7)

= 31 XOR 37

= 00

Plaintext(8) = V(8) XOR H2(8)

= 31 XOR 39

= 00

Plaintext(9) = V(9) XOR H2(9)

= 35 XOR 30

= 00

Plaintext(10) = V(10) XOR H2(10)

= 31 XOR 35

= 00

Plaintext(11) = V(11) XOR H2(11)

= 36 XOR 34

= 00

Plaintext(21) = V(21) XOR H2(21)

= 30 XOR 33

= 00

Plaintext(12) = V(12) XOR H2(12)

= 32 XOR 36

= 00

Plaintext(22) = V(22) XOR H2(22)

= 30 XOR 31

= 00

Plaintext(13) = V(13) XOR H2(13)

= 35 XOR 32

= 00

Plaintext(23) = V(23) XOR H2(23)

= 30 XOR 32

= 00

Plaintext(14) = V(14) XOR H2(14)

= 37 XOR 30

= 00

Plaintext(24) = V(24) XOR H2(24)

= 30 XOR 35

= 00

Plaintext(15) = V(15) XOR H2(15)

= 34 XOR 30

= 00

Karena H2 lebih pendek dari V, maka H2 diulang dari awal

Plaintext(16) = V(16) XOR H2(16)

= 32 XOR 34

= 00

Plaintext(25) = V(25) XOR H2(0)

= 31 XOR 32

= 00

Plaintext(17) = V(17) XOR H2(17)

= 31 XOR 33

= 00

Plaintext(26) = V(26) XOR H2(1)

= 36 XOR 33

= 00

Plaintext(18) = V(18) XOR H2(18)

= 38 XOR 39

= 00

Plaintext(27) = V(27) XOR H2(2)

= 34 XOR 36

= 00

Plaintext(19) = V(19) XOR H2(19)

= 37 XOR 34

= 00

Plaintext(28) = V(28) XOR H2(3)

= 34 XOR 33

= 00

Plaintext(20) = V(20) XOR H2(20)

= 35 XOR 35

= 00

Plaintext(29) = V(29) XOR H2(4)

= 30 XOR 33

= 00

Plaintext(30) = V(30) XOR H2(5)

= 33 XOR 30

= 00

Plaintext(31) = V(31) XOR H2(6)

= 38 XOR 34

= 00

Plaintext(32) = V(32) XOR H2(7)

= 31 XOR 37

= 00

Plaintext(33) = V(33) XOR H2(8)

= 31 XOR 39

= 00

Plaintext(34) = V(34) XOR H2(9)

= 35 XOR 30

= 00

Plaintext(35) = V(35) XOR H2(10)

= 31 XOR 35

= 00

Plaintext(36) = V(36) XOR H2(11)

= 36 XOR 34

= 00

Plaintext(37) = V(37) XOR H2(12)

= 32 XOR 36

= 00

Plaintext(38) = V(38) XOR H2(13)

= 35 XOR 32

= 00

Plaintext(39) = V(39) XOR H2(14)

= 37 XOR 30

= 00

Plaintext(40) = V(40) XOR H2(15)

= 34 XOR 30

= 00

Plaintext(41) = V(41) XOR H2(16)

= 32 XOR 34

= 00

Plaintext(42) = V(42) XOR H2(17)

= 31 XOR 33

= 00

Plaintext(43) = V(43) XOR H2(18)

= 38 XOR 39

= 00

Plaintext(44) = V(44) XOR H2(19)

= 37 XOR 34

= 00

Plaintext(45) = V(45) XOR H2(20)

= 35 XOR 35

= 00

Plaintext(46) = V(46) XOR H2(21)

= 30 XOR 33

= 00

Plaintext(47) = V(47) XOR H2(22)

= 30 XOR 31

= 00

Plaintext =
4953545000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

==> UBAH PLAINTEXT KE KARAKTER

Plaintext (0) = 49 --> I

Plaintext (1) = 53 --> S

Plaintext (2) = 54 --> T

Plaintext (3) = 50 --> P

Plaintext (4) = 00 -->

Plaintext (5) = 00 -->

Plaintext (6) = 00 -->

Plaintext (7) = 00 -->

Plaintext (8) = 00 -->

Plaintext (9) = 00 -->

Plaintext (10) = 00 -->

Plaintext (11) = 00 -->

Plaintext (12) = 00 -->

Plaintext (13) = 00 -->

Plaintext (14) = 00 -->

Plaintext (15) = 00 -->

Plaintext (16) = 00 -->

Plaintext (17) = 00 -->

Plaintext (18) = 00 -->

Plaintext (19) = 00 -->

Plaintext (20) = 00 -->

Plaintext (21) = 00 -->

Plaintext (22) = 00 -->

Plaintext (23) = 00 -->

Plaintext (24) = 00 -->

Plaintext (25) = 00 -->

Plaintext (26) = 00 -->

Plaintext (27) = 00 -->

Plaintext (28) = 00 -->

Plaintext (29) = 00 -->

Plaintext (30) = 00 -->

Plaintext (31) = 00 -->

Plaintext (32) = 00 -->

Plaintext (33) = 00 -->

Plaintext (34) = 00 -->

Plaintext (35) = 00 -->

Plaintext (36) = 00 -->

Plaintext (37) = 00 -->

Plaintext (38) = 00 -->

Plaintext (39) = 00 -->

Plaintext (40) = 00 -->

Plaintext (41) = 00 -->

Plaintext (42) = 00 -->

Plaintext (43) = 00 -->

Plaintext (44) = 00 -->

Plaintext (45) = 00 -->

Plaintext (46) = 00 -->

Plaintext (47) = 00 -->

PESAN ==> IST

CHARLIE MENDAPATKAN PESAN DARI BOB

5. SIMPULAN

5.1 Simpulan

Setelah menyelesaikan tugas akhir ini, penulis menarik beberapa kesimpulan sebagai berikut :

1. Perangkat lunak mampu menampilkan proses kerja dari algoritma kriptografi IBE secara terperinci tahapan demi tahapan dan juga fasilitas pengaturan kecepatan perhitungan serta animasi proses, sehingga dapat digunakan untuk membantu pemahaman algoritma kriptografi IBE

2. Perangkat lunak juga menyediakan fasilitas save yang dapat menyimpan proses kerja dan hasil perhitungan dari algoritma kriptografi IBE, sehingga dapat digunakan untuk membantu pemahaman algortima kriptografi IBE.

5.2 Saran

Penulis ingin memberikan beberapa rekomendasi yang dapat membantu pengembangan perangkat lunak lebih lanjut, antara lain:

1. Dengan menggunakan algoritma kriptografi IBE, pengembangan aplikasi enkripsi dan dekripsi file memungkinkan pengembangan perangkat lunak lebih lanjut.
2. Perangkat lunak dapat ditambahkan beberapa animasi gambar 3D dan efek suara agar proses pembelajaran menjadi lebih menarik.

DAFTAR PUSTAKA

1. Kurniawan. J, 2014, Kriptografi: Keamanan Internet dan Jaringan Komunikasi, Penerbit Informatika, Bandung.

2. Schneier. B, 2006, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, Penerbit John Wiley & Sons, Inc, USA.

3.Jennifer Seberpy, Jojef Pieprzyk, Cryptography: An Introduction to Computer Security.

4.Bruce Schneier, Applied Crytography, Second Edition, John Willey and Sons Inc.

5. http://crypto.stanford.edu/ibe/ Tanggal Akses: 30 April 2025

6.http://crypto.stanford.edu/~dabo/papers/ccaibejour.pdf Tanggal Akses: 30 April 2025