IMPLEMENTASI ENKRIPSI DEKRIPSI ALGORITMA AFFINE CIPHER BERBASIS ANDROID

Sasono Wibowo[1], Florentina Esti Nilawati[2], Suharnawi[3]
[1,2,3]Program Studi Sistem Informasi, Fakultas Ilmu Komputer
Universitas Dian Nuswantoro Semarang
Jl. Nakula I No. 5 – 11 Semarang 50131
Telp. (024)3517261, Fax. (024)3520165
E-mail: sasono@dosen.dinus.ac.id[1], florentina.esti@dsn.dinus.ac.id[2], suharnawi@dsn.dinus.ac.id[3]

Abstrak

Perkembangan Teknologi Informasi yang cukup pesat khususnya dalam bidang komunikasi menjadikan komunikasi sangat mudah namun dalam implementasinya perlu adanya keamanan tentang informasi yang disampaikan. Dalam komunikasi antar orang pasti memiliki pembicaraan informasi yang bersifat privat atau orang lain tidak boleh tahu tentang pembicaraan yang terjadi. Diperlukannya keamanan untuk menjaga kerahasiaan informasi pada saat komunikasi. Masyarakat lebih sering menggunakan komunikasi dengan telepon seluler karena dinilai mudah dibawa dan tidak repot menggunakannya. Kriptografi yang biasa dikenal sebagai ilmu yang mempelajari bagaimana cara menyembunyikan pesan bisa diterapkan dalam aplikasi pada telepon seluler sebagai contoh smartphone android. Dengan mengimplementasikan algoritma affine cipher maka aplikasi yang akan dibuat bisa mengubah isi pesan yang ada dan dapat mengamankan informasi yang ada. Algoritma affine cipher merupakan perkembangan dari algoritma caesar dimana algoritma affine cipher menggunakan dua kunci. Dengan mengimplementasikan algoritma affine cipher ke dalam android maka diharapkan kita bisa menyimpan informasi dari siapapun tanpa terbaca.

Kata Kunci : *Kriptografi, Affine Cipher, android, Implementasi, Informasi*

Abstract

The rapid development of information technology, especially in the field of communication makes communication very easy but in the implementation needs security of the information submitted. In the communication between people must have a conversation that is private information or other people may not know about the conversation that occurred. Security needed to maintain the confidentiality of information at the time of communication. People are much more frequent use of communication with mobile phones because it is considered easy to carry and do not bother using it. Cryptography is commonly known as the study of how to hide the message can be applied in applications on mobile phones, as an example is application in android smartphone. With the affine cipher algorithm implements the application to be made to change the content of any message and can safeguard the information. Affine cipher algorithm is the development of Caesar Algorithm which affine cipher algorithm uses two keys. By implementing affine cipher algorithm into android, it is expected that we can keep the privacy of the stored information.

Keywords: *Cryptography, Affine Cipher, android, Implementation, Information*

1. PENDAHULUAN

Perkembangan teknologi komunikasi bisa dilihat dari alat komunikasi berupa mesin fax, mesin telegram, telepon, pager, telepon seluler, dll. Dengan adanya teknologi tersebut membuat orang tidak mengenal jarak dan waktu

untuk terus berkomunikasi. Dalam berkomunikasi pasti ada halnya suatu informasi tersebut sangat penting dan rahasia. Komunikasi secara visual atau dengan teks bisa dibilang tingkat keamanannya masih kurang. Dilihat dari apakah pesan tersebut akan dibaca orang lain atau tidak. Untuk mengirimkan pesan yang bernilai penting dan rahasia, dibutuhkan keamanan dalam teks tersebut.

Telah banyak dilakukan penelitian dalam upaya mengamankan suatu pesan atau informasi penting dengan berbagai cara namun cara tersebut ternyata dianggap belum cukup dalam mengamankan suatu pesan atau informasi karena adanya peningkatan kemampuan komputasi. Dari sinilah timbul suatu usaha untuk mengembangkan sistem yang mampu mendukung kebutuhan dari dua aspek keamanan informasi, yaitu secrecy (perlindungan terhadap kerahasiaan data informasi) dan authenticity (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan).

Masalah pengiriman pesan ini biasanya terdapat pada suatu instansi baik negeri maupun swasta, misalnya saja ada seorang karyawan bagian rekrutmen disuatu perusahaan ingin mengirimkan pesan ke bagian HRD, karena pesan yang dikirim bersifat rahasia maka dibutuhkan pengenkripsian pesan tersebut.

Pengenkripsian data atau informasi sangatlah penting guna menunjang keamanan informasi dalam suatu instansi baik negeri maupun swasta, karena bisa memberikan jaminan keamanan pesan yang akan diberikan kepada orang atau lembaga yang dituju. Oleh sebab itu, enkripsi sangatlah dibutuhkan bagi user (pengguna) jika ingin data atau informasi yang dimilikinya terjamin kerahasiaannya.
Pada zaman Romawi Kuno kriptografi sudah digunakan untuk mengirimkan pesan rahasia oleh Julius Caesar. Sandi Affine merupakan bentuk pengembangan dari sandi Caesar dengan menggunakan dua kunci dan aritmatik modulo. Membuat aplikasi android dengan mengimplementasikan ilmu kriptografi menggunakan sandi Affine menjadi salah satu cara dalam menjaga kerahasiaan informasi dan pesan penting.

1.1 Pengertian Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Kriptografi merupakan cabang dari ilmu matematika yang memiliki banyak fungsi dalam pengamanan data. Kriptografi memiliki proses mengambil pesan atau message dan menggunakan beberapa fungsi untuk menggenerasi materi kriptografis [1].

1.2 Konsep Kriptografi

Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni: [2]

- Confidentiality (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
- Data integrity (keutuhan data) yaitu layanan yang mampu

mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
- Authentication (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
- Non-repudiation (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi:
• Plaintext (P) adalah pesan yang hendak dikirimkan (berisi data asli).
• Ciphertext (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
• Enkripsi (E) adalah proses pengubahan plaintext menjadi ciphertext.
• Dekripsi (D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal/asli.
• Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.
Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah plaintext menjadi ciphertext (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti [3].

Peranan kunci sangatlah penting dalam proses enkripsi dan dekripsi (disamping pula algoritma yang digunakan) sehingga kerahasiaannya sangatlah penting, apabila kerahasiaannya terbongkar, maka isi dari pesan dapat diketahui.

Secara matematis, proses enkripsi merupakan pengoperasian fungsi E (enkripsi) menggunakan e (kunci enkripsi) pada P (plaintext) sehingga dihasilkan C (ciphertext), notasinya :

$$Ee(P) = C \quad (1)$$

Sedangkan untuk proses dekripsi, merupakan pengoperasian fungsi D (dekripsi) menggunakan d (kunci dekripsi) pada C (ciphertext) sehingga dihasilkan P (plaintext), notasinya :

$$Dd(C) = P \quad (2)$$

Sehingga dari dua hubungan diatas berlaku :

$$Dd(Ee(P)) = P \quad (3)$$

1.3 Affine Cipher

Affine cipher adalah perluasan dari metode Caesar cipher yang menggunakan teknik substitusi yang menggunakan fungsi liniear ap+b untuk enkripsi teks asli p dan a-1c-b untuk dekripsi teks sandi c pada Z26. Kunci pada sandi Affine adalah 2 integer yaitu a dan b. Nilai a yang dapat dipakai adalah anggota elemen pada Z26 yang memiliki invers yaitu yang memenuhi gcd(a,26) = 1 [4].

Proses Enkripsi Affine Cipher adalah sebagai berikut. Affine cipher merupakan sandi yang bekerja secara subtitusi. Pada affine cipher terdapat abjad sejumlah m, yang yaitu rentang m-1, maksudnya adalah awal abjad yaitu huruf “A” bernilai 0, huruf kedua “B” bernilai 1, dan seterusnya hingga huruf terakhir dalam abjad yaitu huruf “Z” bernilai 25 [5][6].

Adapun rumus enkripsi dengan menggunakan affine cipher pada satu huruf plaintext menjadi satu huruf ciphertext adalah sebagai berikut:

$$E(x) = (ax + b) \bmod m, \quad (4)$$

Dimana m adalah ukuran abjad, ini berarti modulus m adalah modulus dari ukuran abjad, sedangkan jumlah abjad dalam rentang affine cipher adalah 25, maka modulus m adalah modulus 25. Sedangkan a adalah bilangan yang harus dipilih secara bebas, namun memiliki syarat haruslah coprime dengan nilai m, artinya harus memiliki nilai faktor yang positif.

Proses Dekripsi Affine Cipher adalah sebagai berikut. Fungsi dekripsi affine cipher adalah:

$$D(x) = a\text{-}1(x\text{-}b) \bmod m, \quad (5)$$

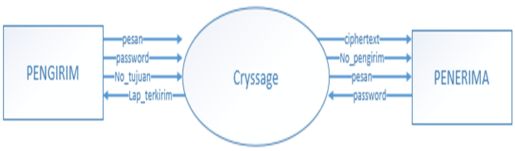
a-1 adalah invers perkalian a modulus m. Yaitu, memenuhi persamaan:

$$1 = aa\text{-}1 \bmod m. \quad (6)$$

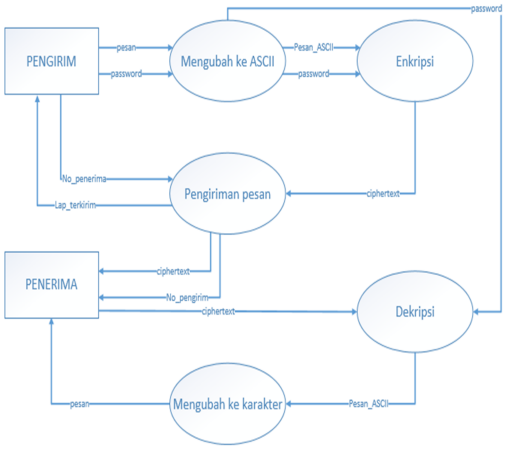
Invers perkalian a hanya ada jika a dan m adalah coprime. Jika tidak maka proses algoritma akan terhenti [7][8][9][10].

2. METODE

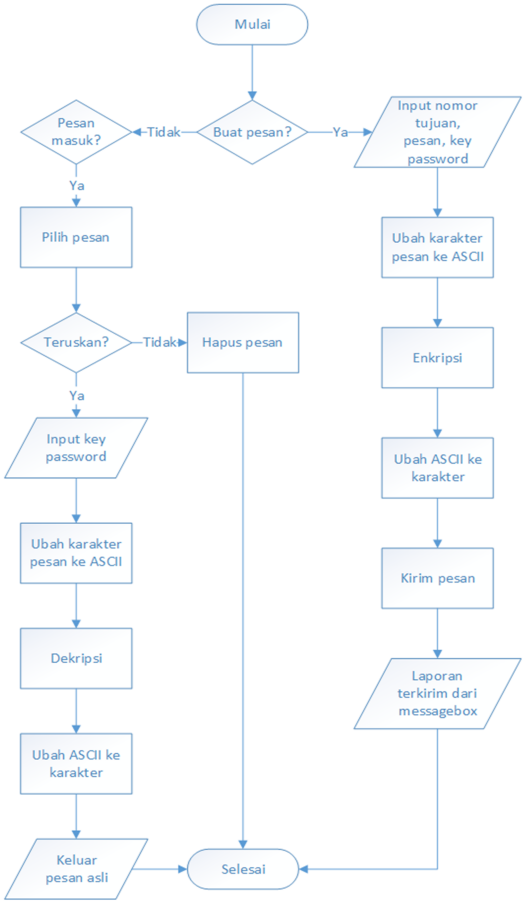
Adapun diagram context dari pemodelan dari Enkripsi Deskripsi Algoritma Affine Chiher digambarkan pada Gambar 1,2 dan 3 [11].



Gambar 1. Context Diagram Aplikasi Cryssage

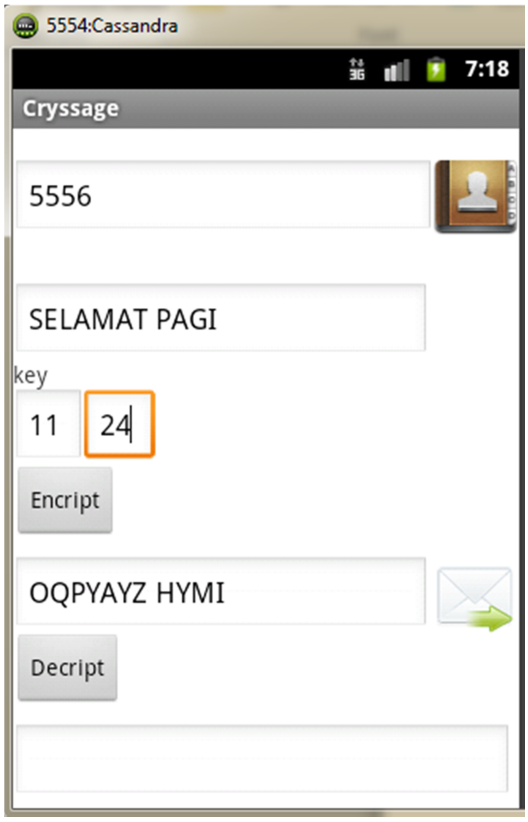


Gambar 2. Data Flow Diagram Aplikasi Cryssage



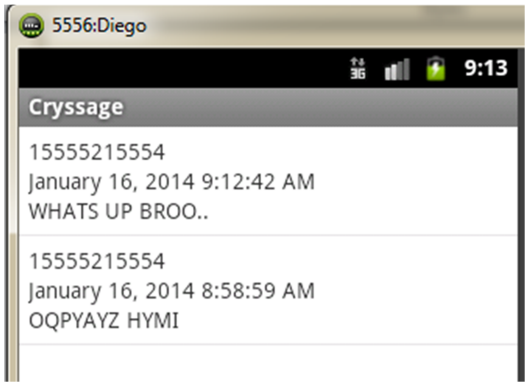
Gambar 3. Flowchart Aplikasi Cryssage

3. HASIL DAN PEMBAHASAN



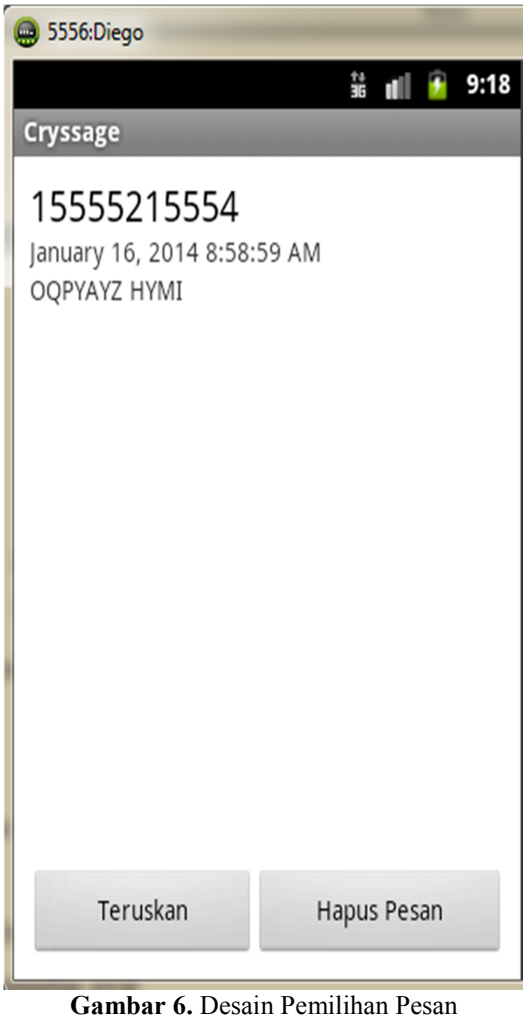
Gambar 4. Desain Proses Pengiriman dan Enkripsi Pesan

Pesan yang masuk akan muncul di tampilan listpesan. Pada proses ini semua pesan yang diterima bisa dilihat di listpesan dan akan terhubung ke lihatpesan saat user memilih pesan yang ingin dibaca.



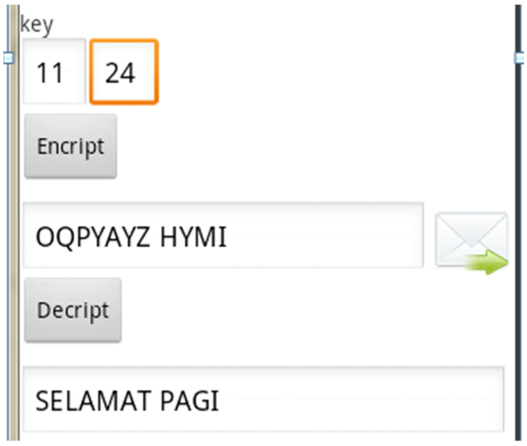
Gambar 5. Desain Kotak Pesan Masuk Aplikasi Cryssage

User dapat memilih pesan yang masuk dari beberapa pesan masuk yang ada sehingga user dapat membaca pesan secara detail. Pesan yang dipilih dapat diteruskan untuk melakukan proses dekripsi pesan atau pesan dapat dihapus.



Gambar 6. Desain Pemilihan Pesan

Pesan yang dipilih user dapat dilakukan proses dekripsi pesan dengan memasukkan key password yang benar sehingga pesan asli akan muncul.



Gambar 7. Desain Proses Dekripsi Pesan

Perhitungan manual untuk proses enkripsi dijelaskan pada Gambar 8 berikut.

Pesan : SELAMATPAGI
ASCII : 83 69 76 65 77 65 84 80 65 71 73
Konversi rumus (ASCII – 65) menjadi nilai array
Nilai array : 18 4 11 0 12 0 19 15 0 6 8
Key 1 = 11
Key 2 = 24
P1 = 18 → C1 = 11.18 + 24 = 222 (mod 26) = 14
P2 = 4 → C2 = 11.4 + 24 = 68 (mod 26) = 16
P3 = 11 → C3 = 11.11 + 24 = 145 (mod 26) = 15
P4 = 0 → C4 = 11.0 + 24 = 24 (mod 26) = 24
P5 = 12 → C5 = 11.12 + 24 = 156 (mod 26) = 0
P6 = 0 → C6 = 11.0 + 24 = 24 (mod 26) = 24
P7 = 19 → C7 = 11.19 + 24 = 233 (mod 26) = 25
P8 = 15 → C8 = 11.15 + 24 = 189 (mod 26) = 7
P9 = 0 → C9 = 11.0 + 24 = 24 (mod 26) = 24
P10 = 6 → C10 = 11.6 + 24 = 90 (mod 26) = 12
P11 = 8 → C11 = 11.8 + 24 = 112 (mod 26) = 8
Nilai array : 14 16 15 24 0 24 25 7 24 12 8
Konversi rumus (nilai array + 65) menjadi ASCII
ASCII : 79 81 80 89 65 89 90 72 89 77 73
Ciphertext : OQPYAYZHYMI

Gambar 8. Perhitungan Untuk Proses Enkripsi

Sedangkan untuk perhitungan manual proses dekripsi dijelaskan pada Gambar 9 berikut.

Ciphertext : O Q P Y A Y Z H Y M I
ASCII : 79 81 80 89 65 89 90 72 89 77 73
Konversi rumus (ASCII – 65) menjadi nilai array
Nilai array : 14 16 15 24 0 24 25 7 24 12 8
Key 1 = 11
Key 2 = 24
C1 = 14 → P1 = 19.((14 + 26)–24) = 304 (mod 26) = 18
C2 = 16 → P2 = 19.((16 + 26) – 24) = 342 (mod 26) = 4
C3 = 15 → P3 = 19.((15 + 26) – 24) = 323 (mod 26) = 11
C4 = 24 → P4 = 19.((24 + 26) – 24) = 494 (mod 26) = 0
C5 = 0 → P5 = 19.((0 + 26) – 24) = 38 (mod 26) = 12
C6 = 24 → P6 = 19.((24 + 26) – 24) = 494 (mod 26) = 0
C7 = 25 → P7 = 19.((25 + 26) – 24) = 513 (mod 26) = 19
C8 = 7 → P8 = 19.((7 + 26) – 24) = 171 (mod 26) = 15
C9 = 24 → P9 = 19.((24 + 26) – 24) = 494 (mod 26) = 0
C10 = 12 → P10 = 19.((12 + 26) – 24) = 266 (mod 26) = 6
C11 = 8 → P11 = 19.((8 + 26) – 24) = 190 (mod 26) = 8
Nilai array : 18 4 11 0 12 0 19 15 0 6 8
Konversi rumus (nilai array + 65) menjadi ASCII
ASCII : 83 69 76 65 77 65 84 80 65 71 73
Pesan : SELAMAT PAGI

Gambar 9. Perhitungan Untuk Proses Dekripsi

4. KESIMPULAN

Kesimpulan yang didapat dari penelitian ini adalah sebagai berikut :

1. Algoritma yang dibuat mengunakan kombinasi kunci yang sulit terprediksi, dikarenakan menggunakan kombinasi dua kunci yang berbeda.
2. Aplikasi Cryssage ini bisa digunakan untuk melakukan enkripsi pesan dan mengirimnya ke nomor tujuan penerima pesan.
3. Aplikasi dibuat sesederhana mungkin, sehingga user bisa dengan mudah mengenali setiap fungsi dari tombol-tombol yang digunakan dalam aplikasi ini.
4. Aplikasi Cryssage bisa digunakan oleh user dalam lingkup umum yang membutuhkan keamanan informasi melalui sms dan mencegah orang yang tidak berkenan untuk mengetahui informasi yang telah dikirim user kepada penerima.

DAFTAR PUSTAKA

[1] Forouzan, Behrouz A. 2009. Cryptography and network security. Mcgraw-hill.

[2] Sadikin, Rifki. 2012. Kriptografi Untuk Keamanan Jaringan. Andi.
[3] Menezes Alfred, Oorschot Paul Van and Vanston Sean, 1996. Handbook of Applied Cryptography, CRC Press.
[4] Hamdani. Kriptografi menggunakan metode affine. http: // hamdani. blog.ugm.ac.id /2011 /07 /07 / kriptografi-untuk-text-message-menggunakan-metode - affine. Tanggal akses 25 Desember 2013.
[5] Mkyong. How to convert character to ascii in java. http://www. mkyong.com/java/how-to-convert-character-to-ascii-in-java. Tanggal akses 17 Desember 2013.
[6] Rauf, ruzlan akba. Kode ascii lengkap. http://informatikakba-ruzlan.blogspot.com/2013/05/kode-ascii-lengkap.html. Tanggal akses 14 Desember 2013.
[7] Y. Kurniawan. 2004. Kriptografi Keamanan Internet dan Jaringan Komunikasi. Informatika. Bandung.
[8] B Schneier. 1996. Applied Cryptography. John Wiley and Sons. Inc.New York.
[9] T. Heriyanto. 1999. Pengenalan Kriptografi. Internet.
[10] J. Chai, M. Leung, M. Ducott, W. Yuen. 2001. Cryptography on the Internet. Computer Communications and Networking ENG SC546.