BAB II. LANDASAN TEORI

2.1 Kriptografi

kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Kriptografi juga menjadi salah satu syarat penting dalam keamanan teknologi informasi dalam pengiriman pesan penting dan rahasia. Kriptografi (*cryptography*) berasal dari bahasa Yunani: "*cryptos*" yang artinya "*secret*" (rahasia) dan "*graphein*" yang artinya "*writing*" (tulisan). Jadi kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*cryptography is the art and science of keeping message secure*) (Munir, 2008).

Kriptografi penting dalam dunia teknologi informasi saat ini terutama dalam bidang komputer yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi. Kriptografi juga menjadi salah satu syarat penting dalam keamanan teknologi informasi dalam pengiriman pesan penting dan rahasia. Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah kriptografi. Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi. [1]

Algoritma kriptografi terdiri dari tiga fungsi dasar yaitu:

1. Enkripsi: merupakan hal yang sangat penting dalam kriptografi. merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut *plaintext*, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cypher* atau kode. Sama halnya dengan kita tidak mengerti akan sebuah kata maka kita akan melihatnya di dalam kamus atau daftar istilah. Beda halnya dengan enkripsi. untuk mengubah teks-asli ke bentuk teks-kode kita menggunakan algoritma yang dapat mengkodekan data yang kita inginkan.
2. Dekripsi: merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks-asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.

3. Kunci: yang dimaksud di sini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci privat (*private key*) dan kunci umum (*public key*). [2]

2.2 Algoritma RSA

Dari banyak algoritma kriptografi asimetris yang ada, algoritma yang paling populer adalah RSA. Algortima RSA dibuat oleh tiga orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun 1976. Nama RSA merupakan singkatan dari nama tiga orang penemunya, yaitu *Rivest*, *Shamir*, dan *Adleman*. Algoritma RSA melakukan pemfaktoran bilangan yang sangat besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Algoritma RSA memiliki besaran-besaran sebagai berikut:

a. p dan q bilangan prima (rahasia).
b. n = p * q (tidak rahasia).
c. φ (n) = (p – 1)(q – 1) (rahasia)
d. e (kunci enkripsi) (tidak rahasia) Syarat: PBB(e, φ (n)) = 1
e. d (kunci dekripsi) (rahasia) d dihitung dari d * e-1 mod (φ (n)) / (d.e) mod φ = 1
f. m (*plainteks*) (rahasia)
g. c (*cipherteks*) (tidak rahasia)

Pembangkitan kunci :

a. Pilih dua bilangan prima, p dan q (rahasia)
b. Hitung n = p q. Besaran n tidak perlu dirahasiakan.
c. Hitung φ (n) = (p – 1)(q – 1).
d. Pilih sebuah bilangan bulat untuk kunci publik, sebut namanya e, yang relatif prima terhadap φ (n) / dengan syarat e > 1, dan FPB (e, φ (n)) = 1.
e. Hitung kunci dekripsi, d, dengan syarat (d.e) mod φ = 1

Hasil dari algoritma di atas:

a. Kunci publik adalah pasangan (e, n)
b. Kunci privat adalah pasangan (d, n). [3]

2.3 *TCP/IP*

Lapisan transpor atau *transport layer* adalah lapisan keempat dari model referensi jaringan OSI. Lapisan transpor bertanggung jawab untuk menyediakan layanan-layanan yang dapat diandalkan kepada protokol-protokol yang terletak di atasnya. Layanan yang dimaksud antara lain:

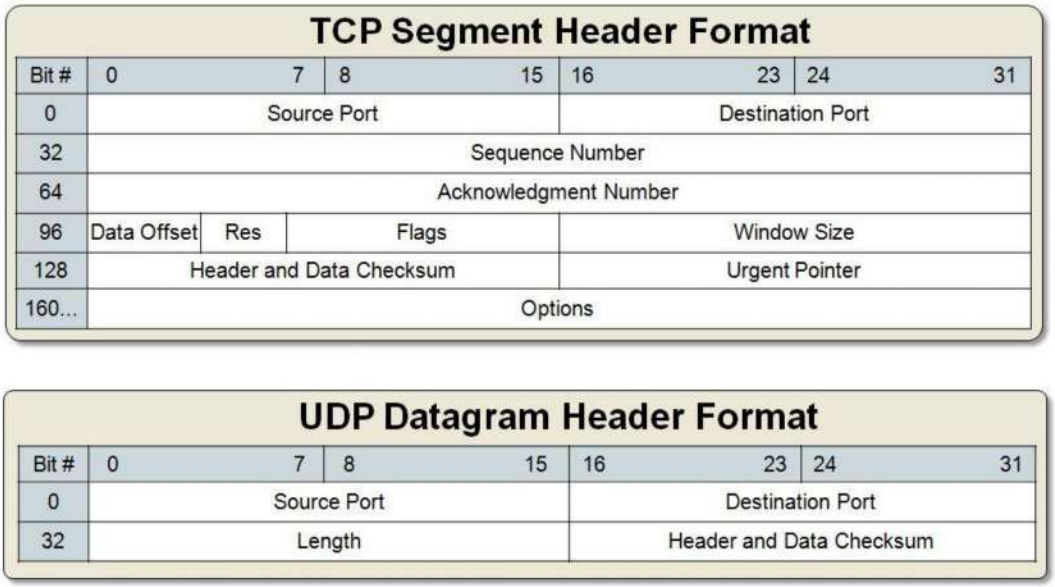
Mengatur alur *flow control* untuk menjamin bahwa perangkat yang mentransmisikan data tidak mengirimkan lebih banyak data daripada yang dapat ditangani oleh perangkat yang menerimanya.

Salah satu Protokol Transport yang akam di implementasikan adalah TCP/IP (singkatan dari *Transmission Control Protocol/Internet Protocol*) yang diterjemahkan menjadi Protokol Kendali Transmisi/Protokol Internet, yang merupakan gabungan dari protokol TCP (*Transmission Control Protocol*) dan IP (*Internet Protocol*) sebagai sekelompok protokol yang mengatur komunikasi data dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan internet yang akan memastikan pengiriman data sampai ke alamat yang dituju. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini, karena protokol ini mampu bekerja dan diterapkan pada lintas perangkat lunak dalam berbagai sistem operasi Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP *stack* dapat dilihat pada gambar 2.1:

<table>
<tr><td>OSI Model</td><td>DoD Model</td><td colspan="7">TCP/IP Suite of Protocols</td></tr>
<tr><td>Application
Presentation
Session</td><td>Application
(Port)</td><td>HTTP
80</td><td>SNMP
161
162</td><td>FTP
20
21</td><td>TFTP
69</td><td>SMTP
25</td><td>Telnet
23</td><td>NNTP
119</td></tr>
<tr><td>Transport</td><td>Host to Host</td><td colspan="3">TCP</td><td colspan="4">UDP</td></tr>
<tr><td>Network</td><td>Internet</td><td colspan="2">ICMP</td><td colspan="4">IP
ARP</td></tr>
<tr><td>Data Link
Physical</td><td>Network
Access</td><td colspan="6">Network Devices</td></tr>
</table>

Gambar 2. 1 TCP/IP *Port*

Transport Control Protocol (TCP): TCP menyediakan fitur *error control* dan *flow control* yang diperluas untuk memastikan data terkirim dengan sempurna. TCP termasuk *connection-oriented protocol* [4] dapat dilihat pada gambar 2.2:



TCP Segment Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

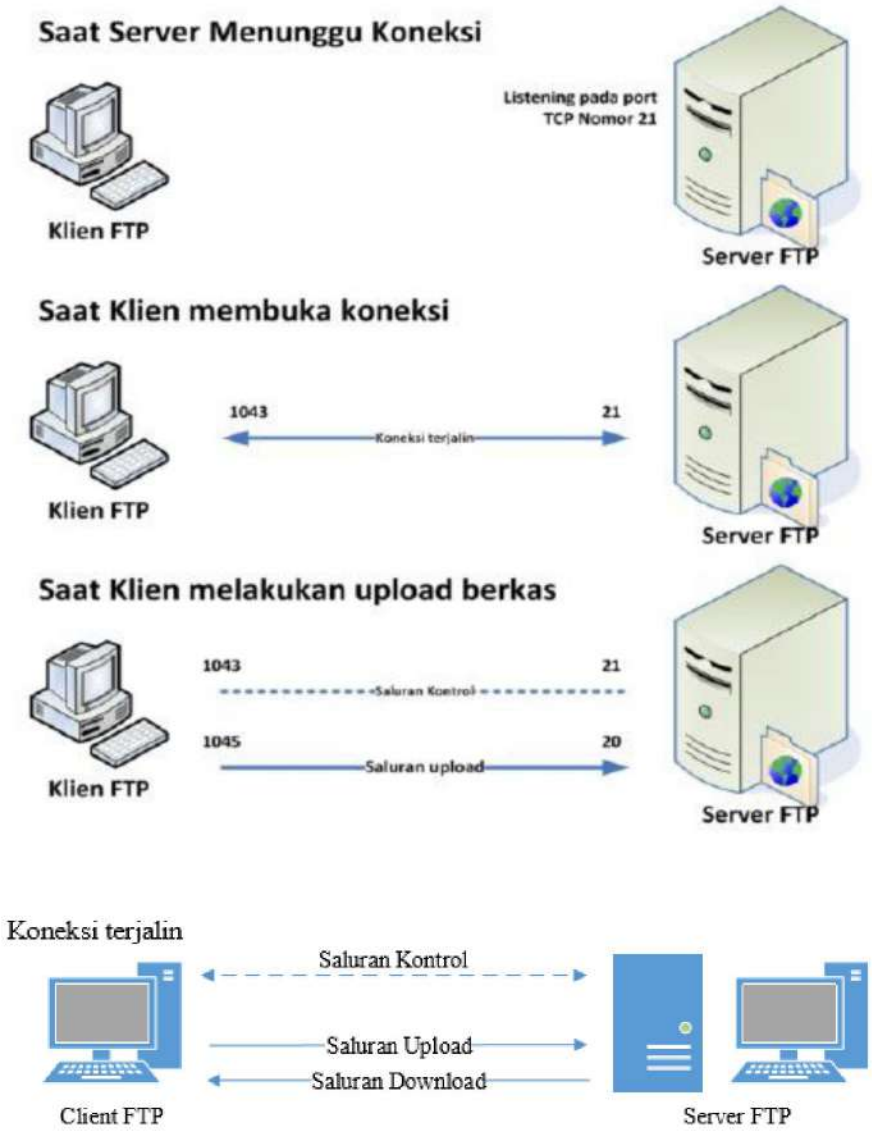
UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

Gambar 2. 2 TCP *Header Format*

2.4 *File Transfer Protocol* (FTP)

File Transfer Protocol (FTP) adalah suatu protokol yang berfungsi untuk melakukan pertukaran *file* antar *Node* dalam suatu jaringan yang menggunakan koneksi TCP. Dua hal yang penting dalam FTP adalah FTP *Server* dan FTP *Client*. FTP *server* adalah suatu *server* yang menjalankan *software* yang berfungsi untuk memberikan layanan tukar menukar *file* dimana *server* tersebut selalu siap memberikan layanan FTP apabila mendapat permintaan (*request*) dari FTP *client*. [5] Selain kelebihan yang ada pada *protocol* aplikasi ini terdapat kelemahan dalam aplikasi FTP yaitu dimana segmen *datagram* dikirimkan secara langsung tanpa adanya keamanan penyandian pesan atau kriptografi sehingga proses komunikasi yang ada sangat rawan terhadap penyadapan data oleh pihak ke tiga dapat dilihat pada gambar 2.3:



Gambar 2. 3 Ilustrasi koneksi *Port* FTP

2.5 JAVA

Java adalah bahasa pemrograman yang dapat dijalankan di berbagai komputer termasuk telepon genggam. Bahasa ini awalnya dibuat oleh *James Gosling* saat masih bergabung di *Sun Microsystems* saat ini merupakan bagian dari *Oracle* dan dirilis tahun 1995. Bahasa ini banyak mengadopsi sintaksis yang terdapat pada *C* dan *C++* namun dengan sintaksis model objek yang lebih sederhana serta dukungan rutin-rutin aras bawah yang minimal. Aplikasi-aplikasi berbasis java umumnya dikompilasi kedalam *p-code bytecode* dan dapat dijalankan pada berbagai *Java Virtual Machine* (JVM). Java merupakan bahasa pemrograman yang bersifat umum/non-spesifik

general purpose, dan secara khusus didisain untuk memanfaatkan dependensi implementasi seminimal mungkin. Karena fungsionalitasnya yang memungkinkan aplikasi java mampu berjalan di beberapa *platform* sistem operasi yang berbeda, *Java* dikenal pula dengan slogannya, "Tulis sekali, jalankan di mana pun". Saat ini *Java* merupakan bahasa pemrograman yang paling populer digunakan, dan secara luas dimanfaatkan dalam pengembangan berbagai jenis perangkat lunak aplikasi ataupun aplikasi.

2.6 *Java Development Kit* (JDK)

Java adalah sebuah teknologi yang diperkenalkan *Sun Microsystems* pada pertengahan tahun 1990. Menurut *Sun* Java adalah nama untuk sekumpulan teknologi untuk membuat dan menjalankan perangkat lunak pada komputer *standalone* ataupun pada lingkungan jaringan. Untuk membuat program *Java* dibutuhkan *compiler* dan *intrepeter* untuk program *Java* berbentuk *Java Development Kit* (JDK) yang diproduksi oleh *Sun Microsystem*. (Safaat H, 2011:5).