# BAB II

# DASAR TEORI

## Teori Tentang Permasalahan

Pada bab ini akan dibahas menganai kriptografi dimulai dari definisi kriptografi, sejarah kriptografi, sistem kriptografi klasik, sistem kriptografi kunci simetris juga sistem kriptografi Advanced Encryption System (AES), sistem kriptografi kunci asimetris terutama sistem kriptografi Rivest Shamir Adleman (RSA), sistem kriptografi hybrid, juga teori-teori bilangan untuk kriptografi kunci publik dan kunci privat.

1. **Kriptografi**

Kata cryptography berasal dari bahasa Yunani: krupto (hidden atau secret) dan grafh (writing) Artinya “secretwriting”. Menurut Schneiner “Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (message).” [Schneier,1996]. Sedangkan menurut Menez bahwa “Kriptografi adalah ilmu yang mempelajari teknik - teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritasdata, sertaotentikasi.”

1. **Sistem Kriptografi RSA**

RSA merupakan algoritma kriptografi asimetris karena menggunakan dua kunci, yaitu kunci publik dan kunci pribadi. Ada tiga algoritma dalam kriptografi RSA, yaitu pembangkitan kunci, proses enkripsi, dan proses dekripsi. Algoritma ini memiliki tingkat keamanan yang terletak pada sulitnya memfaktorkan sebuah bilangan besar menjadi dua buah bilangan prima. Kelemahan dari algoritma kriptografi RSA adalah waktu yang dibutuhkan untuk melakukan proses pembangkitan kunci, enkripsi dan dekripsi lambat. Sedangkan kelebihannya terletak pada sulitnya memecahkan kunci dan penggunaan kunci yang lebih efektif.

1. **Prosedur pada Sistem Kriptografi RSA**
2. **Proses Enkripsi pada Sistem Kriptografi RSA**
3. **Proses Dekripsi pada Sistem Kriptografi RSA**
4. **Sistem Kriptografi AES**

AES adalah algoritma kriptografi berbasis chipertext simetrik yang dapat mengenkripsi dan dekripsi video surveillance. AES memiliki sifat cipher yang diharapkan yaitu: tahan menghadapi analisis sandi yang diketahui serta fleksibel digunakan dalam berbagai perangkat keras dan perangkat lunak. Algoritma ini menggunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi.

1. **Prosedur pada Sistem Kriptografi AES**
2. **Proses Enkripsi pada Sistem Kriptografi AES**
3. **Proses Dekripsi pada Sistem Kriptografi AES**
4. **Sistem Kriptografi Hibrid**

Kriptografi hibrid melakukan enkripsi secara berlapis. Hal ini secara teori akan membuat pemecahannya menjadi semakin kompleks. Algoritma kriptografi hibrid (hybrid cryptosystem) merupakan gabungan antara kriptografi simetris dan kriptografi asimetris. Permasalahan yang menarik pada bidang keamanan informasi adalah adanya trade off antara kecepatan dengan kenyamanan. Salah satu contohnya adalah bidang kriptografi. Tetapi hal ini dapat diatasi dengan penggunaan kriptografi hibrid. Kriptografi hibrid sering dipakai karena memanfaatkan keunggulan kecepatan pemrosesan data oleh algoritma kriptrografi simetrik dan kemudahan transfer kunci menggunakan algoritma kriptografi asimetrik. Hal ini mengakibatkan peningkatan kecepatan tanpa mengurangi kenyamanan serta keamanan.

1. **Prosedur pada Sistem Kriptografi Hibrid**
2. **Proses Enkripsi pada Sistem Kriptografi Hibrid**
3. **Proses Dekripsi pada Sistem Kriptografi Hibrid**
4. **Bahasa Pemrograman Python**

Python merupakan interpreter bahasa pemrograman tingkat tinggi berbasis objek dengan semantik yang dinamis, dimana bersifat freeware atau perangkat bebas dalam arti sebenarnya, tidak ada batasan dalam penyalinannya atau mendistribusikannya. Lengkap dengan source codenya, debugger dan profiler, antarmuka yang terkandung di dalamnya untuk pelayanan antarmuka, fungsi sistem, antarmuka pengguna grafis (GUI), dan basis datanya. Python dapat digunakan dalam beberapa sistem operasi, seperti kebanyakan sistem UNIX, PCs (DOS, Windows, OS/2), Macintosh, dan lainnya. Pada kebanyakan sistem operasi linux, bahasa pemrograman ini menjadi standarisasi untuk disertakan dalam paket distribusinya.

## Metodologi Yang Digunakan