PENUTUP

KESIMPULAN

Berdasarkan pembahasan, maka dapat diambil kesimpulan sebagai berikut :

1. Kriptografi dapat digunakan untuk mengamankan plainteks yang bersifat rahasia dari pihak-pihak yang tidak berwenang untuk mengetahuinya.
2. Keamanan kriptosistem terletak pada kunci-kunci yang digunakan, baik kunci enkripsi maupun kunci dekripsi, tidak terletak pada algoritma yang dipakai dalam enkripisi dan dekripsi
3. Kriptosistem Kunci Umum menggunakan kunci enkripsi dan kunci dekripsi yang berbeda. Kunci enkripsi yang bersifat publik hanya memerlukan otentikasi atau keaslian yang dapat dilakukan dengan menggunakan sertifikat digital.
4. Keamanan algoritma Rivest-Shamir-Adleman (RSA) terletak pada pemfaktoran nilai modulus n.