

Pre-Test Kriptografi

M. ZAKI RIYANTO
PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UIN SUNAN KALIJAGA YOGYAKARTA
zaki.riyanto@uin-suka.ac.id
<https://zaki.sandimath.web.id>

Sebelum diberikan konsep-konsep yang lebih dalam dari kriptografi, mahasiswa diharapkan sudah memahami motivasi kriptografi, serta konsep dasar teori bilangan dan struktur aljabar yang menyertainya dengan baik. Oleh karena itu, perlu dilakukan pre-test untuk mengetahui tingkat kemampuan mahasiswa sebelum perkuliahan inti dimulai.

Soal Pre-Test:

- (1) Misalkan ada dua pihak yang saling berkomunikasi di dalam kelas, namakan mereka adalah Alice dan Bob. Keduanya biasa berkomunikasi menggunakan surat kertas yang ditulis dengan pensil. Pada suatu ketika, keduanya duduk berjauhan, sehingga untuk berkomunikasi keduanya membutuhkan bantuan temannya, misalkan namanya Oscar. Terkadang Alice dan Bob membicarakan sesuatu yang bersifat rahasia yang hanya boleh diketahui oleh keduanya saja. Tugas Anda adalah: Identifikasi masalah-masalah apa saja yang dapat terjadi apabila komunikasi antara Alice dan Bob dilakukan melalui bantuan Oscar. Bagaimana solusi yang Anda tawarkan untuk menyelesaikan masalah-masalah tersebut? Jelaskan.
- (2) Seperti yang telah kita ketahui bahwa internet merupakan jalur komunikasi umum yang dapat dilewati oleh siapa saja, sehingga sangat rawan terhadap adanya ancaman keamanan informasi. Tugas Anda adalah: Identifikasi masalah-masalah keamanan apa saja yang dapat terjadi apabila komunikasi dilakukan menggunakan internet.
- (3) Jelaskan pengertian kriptografi. Selanjutnya, sebutkan masalah keamanan informasi yang dapat diselesaikan menggunakan kriptografi, serta sebutkan masalah keamanan informasi yang tidak dapat diselesaikan menggunakan kriptografi.

- (4) Diberikan ring $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
- (i) Buatlah dua Tabel Cayley dari \mathbb{Z}_{10} (terhadap operasi penjumlahan dan perkalian modulo 10).
 - (ii) Berdasarkan Tabel Cayley yang telah dibuat, sebutkan elemen dari \mathbb{Z}_{10} yang memiliki invers terhadap operasi perkalian modulo 10.
 - (iii) Hitunglah faktor persekutuan terbesar dari setiap elemen dari \mathbb{Z}_{10} dengan 10.
 - (iv) Hubungan apa yang Anda dapatkan antara memiliki invers terhadap perkalian dengan faktor persekutuan terbesar dengan 10.
- (5) Kemukakan motivasi Anda mengikuti mata kuliah Kriptografi, serta harapan Anda setelah mengikuti mata kuliah ini.