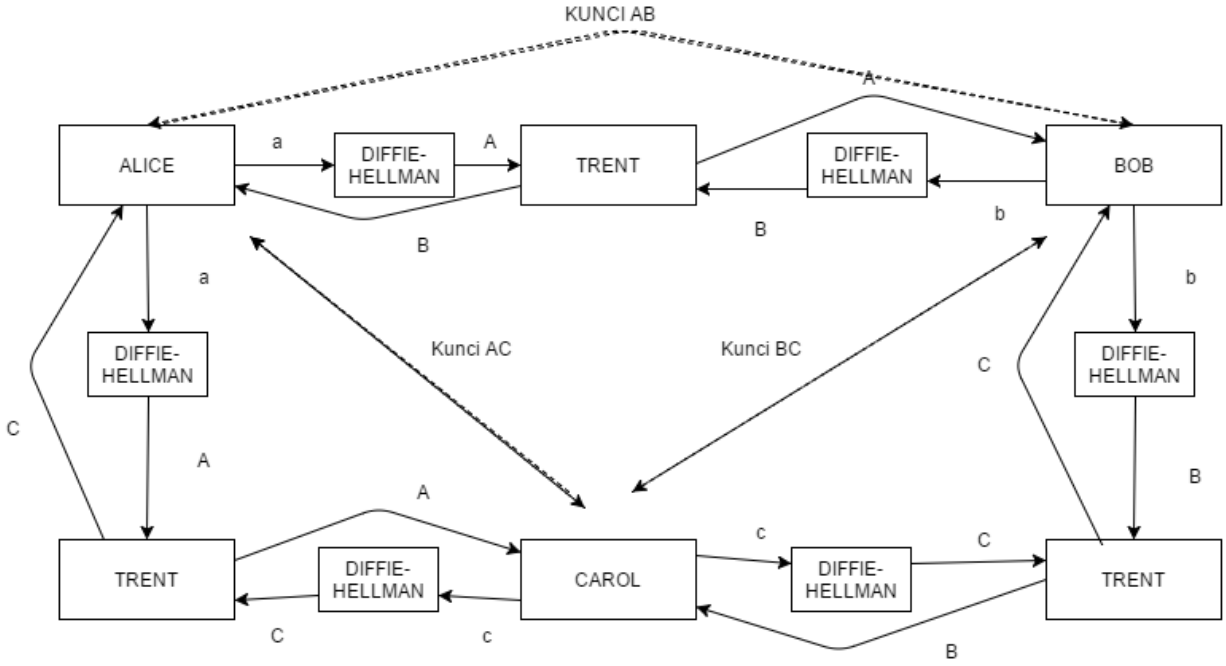
**PROTOKOL KRIPTOGRAFI**

**Oleh Mohamad Ravena Utama (G64140041) &**
**Feby Tri Saputra (G64140047)**




Gambar 1. Protokol Kriptografi Menggunakan Diffie Hellman Key Exchange

Terdapat 3 subjek komunikasi (Alice, Bob, dan Carol) dimana ketika Alice dan Bob berkomunikasi, Carol tidak berhak mengetahui isi informasi atau pesan yang saling dipertukarkan oleh Alice dan Bob. Namun Alice juga dapat berkomunikasi dengan Carol tanpa diketahui oleh Bob. Bob pun dapat berkomunikasi dengan Carol tanpa diketahui oleh Alice. Dalam protocol akan terdapat 3 Trent sebagai perantara di masing-masing komunikasi. Dalam protocol ini digunakan kunci simetris menggunakan *Diffie-Hellman key exchange.* Pada perjanjian pemilihan nilai generator trent akan terlibat sebagai arbitrator. Maka setiap antar komunikasi 2 subjek akan memiliki kunci yang sama sehingga dapat mengirim pesan dan membaca pesan secara aman tanpa diketahui oleh subjek komunikasi yang lain.