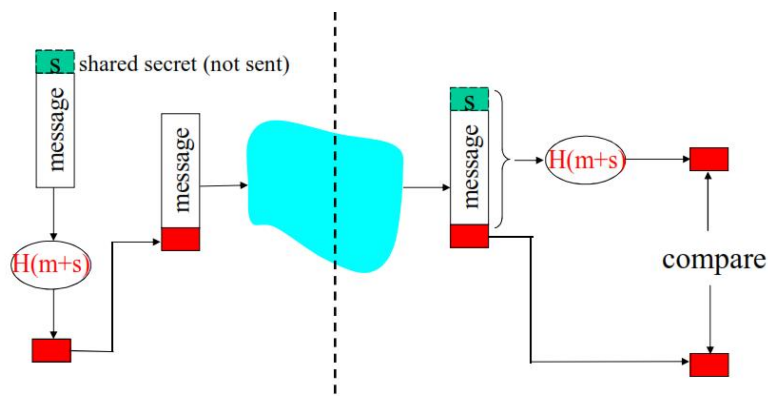


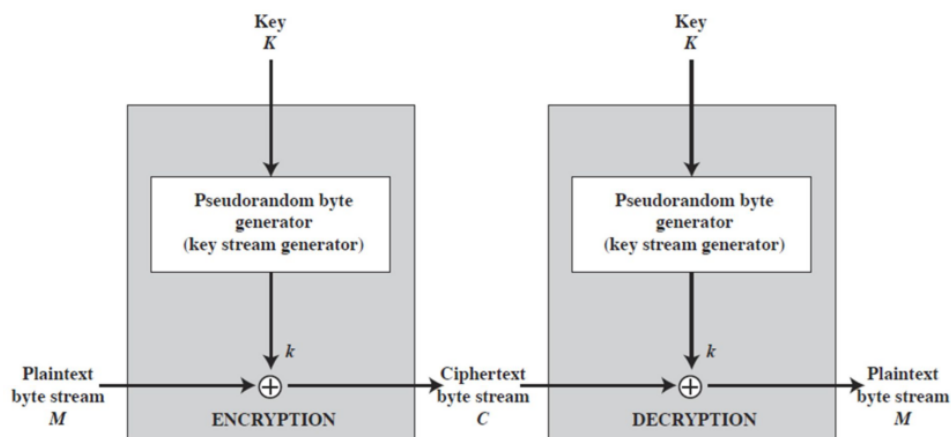
App – kryptera telefonsamtal för mobiler

Dagens samhälle kräver ständigt mer internet uppkoppling. Att prata med mobiltelefoner blir helatiden mer öppet för avlysning, vår integritet och privatliv skjuts åt sidan. Tanken är att utveckla en App som ska strax efter påbörjat samtal **dynamiskt generera och byta engångs krypteringsnyklar** för att kryptera pågående strömningssamtal d.v.s. trafiken.

Med hjälp av t.ex. HMAC (Key-Hashing for Message Authentication) autentisera startade Appar på mobiltelefoner.



Man kan utnyttja samma eller annan teknik för att skicka autogenererade krypteringsnyklar för **Stream ciphers audio kryptering**. Undersök vilka kommersiella nyckelgeneratorer som passar eller utveckla en egen nyckelgenerator (som ska ha hög säkerhet).



Sakib Sistik

Sistik@chalmers.se