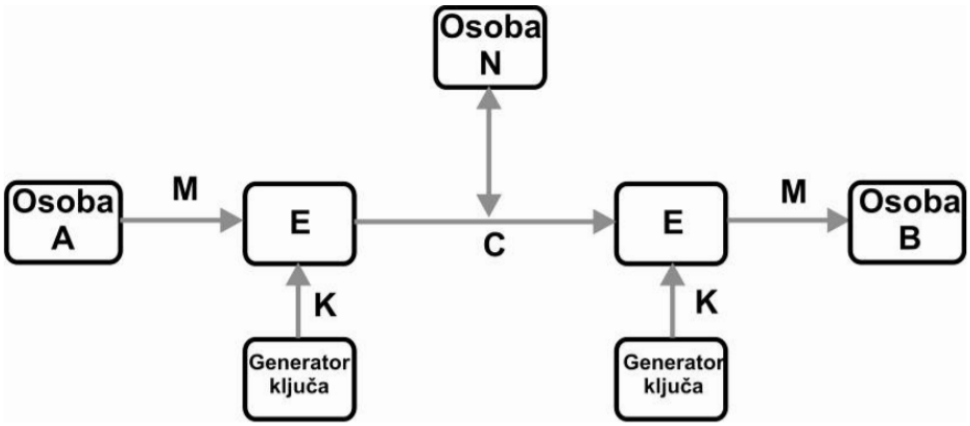
Симетрично шифровање и дешифровање

Основна особина симетричних криптосистема или криптосистема са тајним кључем је да се за криптовање/декриптовање порука користи исти кључ.

На Слици 1 је у виду блокова, приказан принцип рада симетричног криптосистема.

Особа А има за циљ слање поруке М особи В преко незаштићеног комуникационог канала. Особа А најпре генерише поруку М (изворни текст) која се упућује у блок за шифровање Е.

У овом блоку се врши криптовање поруке М уз коришћење кључа К добијеног уз помоћ генератора кључа. На тај начин се креира криптована порука С. Потом се тако добијена порука комуникационим каналом шаље до особе В.



Слика 1: Схема симетричног (де)криптовања

Уколико на каналу за пренос постоји особа N (нападач) може да пресретне криптовану поруку и уколико дође у посед кључа може прочитати или злоупотребити изворну поруку.

Да би се избегле манипулације, обе стране морају држати кључ у тајности, односно кључ се не сме преносити незаштићеним

комуникационим каналом.

За разлику од кључа, криптована порука може да се шаље и по незаштићеном каналу с обзиром на то да садржај изворне поруке може да протумачи само онај корисник који има кључ.

Пример слања кључа различитим комуникационим каналом је када се PIN код за приступ заштићеним Интернет сајтовима (нпр. Банке за увид стања на рачуну) достављају корисницима поштом, а не Интернетом.

Најпознатији алгоритми симетричних криптосистема који се данас користе су: DES, 3DES, DES-CBC,IDEA, RC5, RC6, AES, ...

Предности и недостатци симетричног (де)криптовања

Алгоритми који користе симетрични кључ за криптовање одликују се високом ефикасношћу, што се огледа у кратком времену криптовања порука.

Разлог кратког времена криптовања је употреба кратких кључева. Из тих разлога се ова врста алгоритама користи за криптовање/декриптовање порука велике дужине.

Симетрично криптовање има два основна недостатка. Оба корисника (особа А и особа В) морају поседовати јединствени **симетрични кључ**, те се јавља проблем дистрибуције кључева.

Наиме, корисници који желе да размене поруку претходно морају да се договоре о кључу.

Једини поуздан начин је да се оба корисника физички сретну и изврше размену кључа.

Међутим, често су корисници физички раздвојени и не могу да дођу у непосредан контакт, зато морају да користе неки заштићен канал да би сигурно разменили кључеве. Проблем је то што заштићен канал практично не постоји.

Други проблем који се јавља код симетричних криптосистема је велики број потребних кључева. Ако имамо N људи који желе да користе ову методу криптовања, то захтева **n(n – 1)/2 симетричних кључева**.

На пример за 1 милион људи потребно је 500 милијарди симетричних кључева.

Ради добијања толико великог броја различитих кључева морају се користити кључеви веће дужине.

Тако на пример, дужина кључа од 56 бита је данас на граници довољног с обзиром на то да савремени рачунари могу релативно брзо да открију кључ те дужине.