В чому сутність протоколів автентифікації на основі застосування КАП (MAC). Оцініть ймовірність обману в ІТС при умові застосування КАП (імітo прикладок) з довжиною 16 +4k, де k - номер реєстрації.

Сутність режиму обчислення КАП(MAC). Інформація розбивається на блоки довжиною L бітів. Перший блок перед зашифруванням складається з ключем автентифікації Ка довжиною L бітів. Потім кожен блок зашифрується в блоковому режимі з використанням вихідного ключа зашифрування Кз. Процес повторюється для усіх блоків. При цьому перед зашифруванням Мі блоку він складається з Сі-1 блоком криптограми. Таким чином, останній блок Сп залежить від усіх Мі блоків, ключа автентифікації та ключа зашифрування, тобто:

$$C_n = f\left(M_1, M_2, ..., M_n, K_a, K_з\right).$$

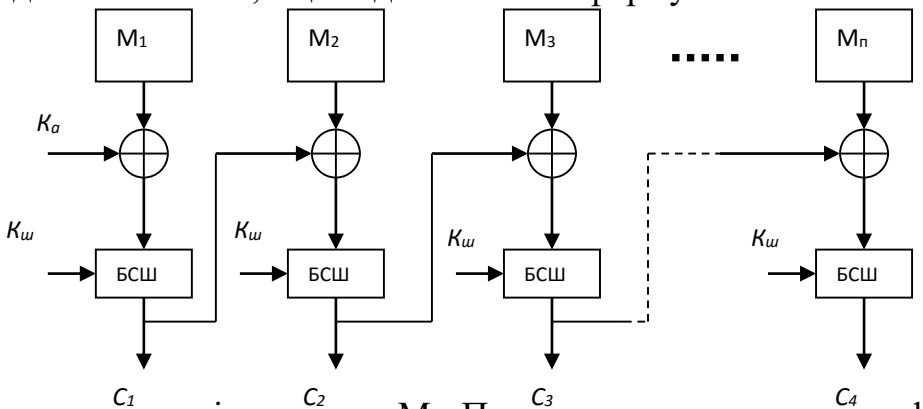
Тому Сп по суті є криптографічною контрольною сумою і може використовуватися як імітоприкладка Імп (згідно з міжнародною термінологією коду автентифікації повідомлень).

Рисунок 1– Алгоритм зашифрування зі зв'язком за шифрованим текстом

Оскільки довжина імітo прикладки дорівнює lімп=128 біт, то граничне значення ймовірності обману можна оцінити як:

$$P_{обм} \geq 2^{-128} \approx 2{,}9 \cdot 10^{-39}.$$

Необхідно зазначити, що одночасно з формуванням імітоприкладки здійснено



зашифрування повідомлення М. При цьому довжина зашифрованого повідомлення дорівнює довжині вихідного повідомлення, тобто автентифікацію здійснено без збільшення довжини зашифрованого повідомлення. Особливістю цього режиму є те, що додатково використовується ключ автентифікації. Якщо повідомлення не має

зашифровуватися, то в цьому випадку до нього додається імітоприкладка і довжина автентифікованого повідомлення збільшується на lб=128 бітів, а саме автентифіковане повідомлення має вигляд {М, Іімп}. Основною перевагою такого методу автентифікації є висока швидкість перетворення і, як наслідок, можливість обчислення значення імітоприкладки в реальному плині часу. Основним недоліком є те, що використовувані ключі Кз та Ка є симетричними, а тому не дозволяють реалізувати захист на основі моделі взаємної недовіри.