**Атака на основі вибраного ШТ**

* Це модель атаки в криптоаналізі, яка передбачає збір інформації крипто аналітиком характерним чином: для обраного ШТ є змога отримати відповідний йому ВТ без додаткових відомостей про секретний ключ. По суті, противник може використовувати систему шифрування для розшифрування необхідного ШТ для отримання відповідного ВТ. Ці часткові відомості можуть надати змогу противнику відновити секретний ключ.

Приклад

Нехай генерал А надсилає повідомлення генералу Б, використовуючи шифр Віженера. Криптоаналітик якимсь чином втрутився в їхній канал зв’язку і замінив зашифроване повідомлення на вибраний ним набір літер («вибраний ШТ»), нехай це буде повідомлення «NLLCJOVFXXHMLY». Генерал Б розшифровує його і в результаті отримує наступне «AKRUWNBXKWNEYX», що для нього не несе жодного змісту. Вважаючи, що ця інформація не має жодної цінності, він телефонує по незакритому каналу генералу А та запитує: «Що Ви мали на увазі під AKRUWNBXKWNEYX? Ви змінили секретний ключ без мого відому?». В цей час Криптоаналітик підслуховує цю розмову і зміг встановити відповідність, що ШТ «NLLCJOVFXXHMLY» відповідає ВТ «AKRUWNBXKWNEYX». Враховуючи використання шифру Віженера, одного розшифрованого повідомлення достатньо, щоб відновити секретний ключ.