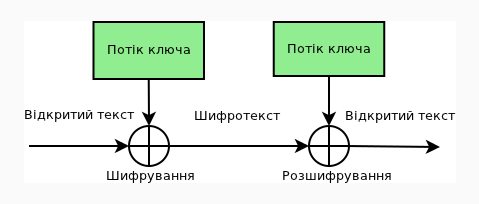
**Потоковий шифр**

– це симетричний шифр, в якому кожен символ ВТ перетворюється в символ ШТ в залежності не тільки від вибраного ключа, але від розміщення даного символу в потоці ВТ.

Схематичне зображення потокового шифру представлене на малюнку.



Генератор гами видає ключовий потік (гаму): . Позначимо потік бітів ВТ . Тоді потік бітів ШТ отримують з допомогою застосування операції XOR: ,  , де .

Розшифрування здійснюється операцією XOR між тою ж гамою і зашифрованим текстом: .

Якщо послідовність бітів гамми не має періоду і обирається випадково, то «зламати» шифр неможливо. Але ключі з довжиною близькою до довжини ВТ, важко використовувати на практиці. Саме через це застосовують ключі меншої довжини (наприклад, 128 біт). З його допомогою генеруються псевдовипадкова гамуюча послідовність. Саме псевдовипадковість гами може бути використана при атаці на потоковий шифр.

**Класифікація потокових шифрів**

Якщо при передачі по каналу зв’язку виникло спотворення одного знаку ШТ, то в цьому випадку всі знаки, прийняті без спотворення, будуть розшифровані правильно. Буде втрата лише одного знака тексту. А у випадку, коли один із знаків ШТ при передачі по каналу зв’язку був втрачений, то це спричинить невірне розшифрування всього тексту, що слідує за втраченим знаком.

В усіх каналах передачі даних є шум. Тому для запобігання втрат інформації вирішують проблему синхронізації шифрування і розшифрування тексту. За способом рішення цієї проблеми шифросистеми поділяються на синхронні і системи із самосинхронізацією.

**Синхронні потокові шифри**

Означення:

Синхронні потокові шифри (СПШ) — шифри, в яких потік ключів генерується незалежно від ВТ і ШТ. При шифруванні генератор потоку ключів видає біти потоку ключів, які ідентичні бітам потоку ключів при дешифруванні. Втрата знаку ШТ приведе до порушення синхронізації між цими двома генераторами і неможливості розшифрування залишкової частини повідомлення. В цій ситуації відправник і адресат повинні повторно синхронізуватися для продовження роботи.

Зазвичай синхронізація здійснюється вставкою в передане повідомлення спеціальних маркерів. Як результат, пропущений при передачі знак призводить до невірного розшифрування лише до тих пір, поки не буде прийнято один із маркерів.

Виконуватись синхронізація повинна так, щоб жодна частина потоку ключів не була повторена. Тому переводити генератор в більш ранній стан не має сенсу.

Позитивні сторони СПШ:

відсутність ефекту розповсюдження помилок (тільки створений біт буде розшифрований невірно);

убезпечують від будь-яких вставок і видалення частин ШТ, адже вони спричинять втрату синхронізації і будуть виявлені.

Негативні сторони СПШ:

Уразливі до змін окремих бітів ШТ. Якщо Криптоаналітику відомий ВТ, то може змінити ці біти так, щоб вони розшифровувались, як йому це потрібно.

**Потокові шифри із самосинхронізацією**

Означення:

Потокові шифри із самосинхронізацією (асинхронні потокові шифри (АПШ)) – шифри, в яких ключовий потік створюється функцією ключа і фіксованим числом знаків ШТ.

Внутрішні стани генератора потоку ключів є функцією попередніх N бітів ШТ. Саме тому розшифровуючий генератор потоку ключів, прийнявши N бітів, автоматично синхронізується із шифруючим генератором.

Реалізація цього режиму проходить наступним чином: кожне повідомлення починається випадковим заголовком довжини N бітів; заголовок шифрується, передаєтся і розшифровується; розшифрування невірне, але після цих N біт обидва генератори будуть синхронізовані.

Позитивні сторони АПШ:

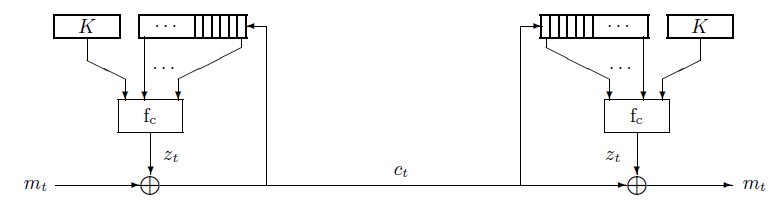
Змішування статистики ВТ. Оскільки кожен знак ВТ впливає на наступний ШТ, статистичні властивості ВТ розповсюджується на весь ШТ. АПШ може бути стійкішим до атак на основі збитковості ВТ, чим СПШ.

Негативні сторони АПШ:

Розповсюдження помилки (кожному неправильному біту ШТ відповідають N помилок у ВТ);

чутливі до злому через повторну передачу.

Схематичне спрощене зображення потокового шифру із самосинхронізацією:



За такого дизайну шифру, наступний знак (біт) ключового потоку  повністю визначається останніми знаками (бітами) ШТ та ключем К. Модель: на вхід деякої функції приходить стан регістру зсуву, що містить символів ШТ, та ключ, як результат отримуємо потоковий символ. Для перших  символів ВТ або ШТ немає, їх емулюють з допомогою ініціалізуючих символів, що називаються вектором ініціалізації IV.