34. В чому сутність та які властивості криптографічного протоколу автентифікації на основі ЕЦП?

криптографічним протоколом автентифікації будемо розуміти криптографічний протокол встановлення достовірності твердження, що об'єкт (суб'єкт) має очікувані властивості. Як правило, достовірність твердження встановлюється з деякою ймовірністю. Тому має сенс застосування такого визначення протоколу автентифікації:

автентифікація об'єкта (суб'єкта) (en entity authentication) – це підтвердження із заданою ймовірністю того, що об'єкт (суб'єкт) є тим, за кого він себе видає.

Для забезпечення захисту у разі автентифікації джерела даних необхідно використовувати ЕЦП. Може також застосовуватись симетричне шифрування, наприклад, у вигляді коду автентифікації повідомлення (імітовставки), або криптографічного контрольного значення від даних, що виготовлені з використанням особистого ключа ЕЦП.

Основні положення надання послуг автентифікації

Загрози автентифікації. Основною задачею автентифікації є надання гарантій справжності ідентифікаційних даних пред'явника (ініціатора комітента).

Загроза типу «маскарад» - Для протистояння загрозам, що належать до такого типу, в процесі автентифікації мають використовуватися спеціальні дані, що пов'язані з деяким механізмом реалізації послуги цілісності (ЕЦП).

Загроза типу «повтор» Зазвичай її використовують у комбінації з іншими атаками, наприклад такими, як атака типу «модифікація». Не всі механізми автентифікації однаково протистоять атакам типу «повтор». Атака типу «повтор» може бути загрозою й для інших послуг безпеки, наприклад неспростовності й автентичності. Механізми автентифікації на основі ЕЦП можна використовувати для протистояння атакам типу «повтор», оскільки ЕЦП забезпечує послугу неспростовності пред'явника.

Загроза типу «підміна» Для захисту проти загроз типу «підміна» краще використовувати послугу цілісності, наприклад з використанням для обміну при автентифікації ЕЦП.

Властивості криптографічного протоколу автентифікації на основі ЕЦП (на прикладі протокола Шнора)

Протокол автентифікації Шнора на основі ЦП є вдосконаленням протоколу Шнора.

Шнор запропонував генерувати запит на основі використання в якості е значення функції гешування від певного повідомлення m. Вказане дозволило реалізувати криптографічний протокол за один прохід, в тому числі з груповою автентифікацією.

При оцінці безпеки протоколу Шнора на основі ЕЦП необхідно відзначити, що пасивна атака порушника (криптоаналітика) має зводитися до знаходження

довгострокового ключа кожного з абонентів X_A та ключа сеансу K_A. Як у першому, так і в другому випадках необхідно розв'язувати задачі дискретного логарифмування в скінченному полі Галуа.

На відміну від трьохетапного протоколу Шнора, протокол Шнора на основі ЦП має такі переваги:

1) для виконання протоколу необхідно виконати тільки один обмін (раунд) (S, r) від А до В;

2) можлива також групова автентифікація А з групою суб'єктів з одночасною перевіркою цілісності повідомлення m.

Проблемними для протоколу Шнора на основі ЦП є такі питання:

1) при помилках в т з великою ймовірністю r' також буде помилковим;

2) якщо m' викривлене, h буде відрізнятись та е не обчислюється.

3) забезпечення неспростовності тільки суб'єкта А.

Основним же недоліком, з точки зору обох протоколів Шнора, є те, що він побудований на основі криптографічного перетворення в скінченному полі Галуа. Для цього випадку складність атаки типу «повне розкриття» має субекспоненційний характер. У той же час його можна вдосконалити, скориставшись перетворенням у групі точок еліптичної кривої, в такому разі складність атаки «повне розкриття» вже буде носити субекспоненційний характер.