23. Сутність атак повне розкриття та їх ефективність відносно асиметричних криптосистем?

полное раскрытие. Противник находит секретный ключ пользователя.

Сутність атаки типу повне розкриття міститься в розв'язку дискретних логарифмічних рівнянь

$$X_A = \log_a Y_A (\mathrm{mod}\, P), \quad (15.32)$$

та

$$X_B = \log_a Y_B (\mathrm{mod}\, P).$$

При розв'язку (2.74) вважається, що загальносистемні параметри (*P*, *a*) та відкриті ключі Y_A та Y_B є відомими.

Якщо криптоаналітик визначить особистий ключ $X_A(X_B)$, то в подальшому він зможе нав'язувати хибні загальні секрети та відповідно хибні повідомлення. Для суттєвого ускладнення можливості нав'язування хибних загальних секретів використовують як довгострокові, так і сеансові загальні секрети.

Загально визнано, що відносно асиметричних криптоперетворень криптографічна стійкість до атак «повне розкриття», коли визначається особистий (конфіденційний) ключ, зводиться до розв'язання деяких математичних задач. Так, для RSA-перетворення задача повного розкриття в основному зводиться до факторизації модуля перетворення, для перетворення в полі Галуа – до дискретного логарифмування в полі Галуа, для перетворення в групі точок еліптичних кривих – до дискретного логарифмування на еліптичній кривій. Далі, для перетворень на гіпереліптичних кривих – до дискретного логарифмування в групі гіпереліптичної кривої, для криптоперетворень у кільцях зрізаних поліномів – до розв'язання певних задач в алгебраїчних решітках. Особливу групу складають задачі криптоаналізу криптоперетворень зі спарюванням точок еліптичних кривих тощо. Зрозуміло, що ці задачі є субекспоненційно або експоненційно складними, особливо для відповідно обґрунтованих вибором параметрів і ключів.