Асиметричні криптосистеми та протоколи
Конспект лекцій

Сергій Яковлєв та група ФІ-33

23 січня 2017 р.

Зміст

Передмова

Лекції жодним чином не редагувались (окрім правок, необхідних для компіляції) та наразі надаються as is.

Розділ 1

Важкооборотні функції та важкооборотні функції із секретом

Розділ 2

Криптографічні геш-функції та схеми цифрового підпису

Розділ 3

Криптосистеми на еліптичних кривих

Розділ 4

Асиметричні криптографічні протоколи

4.1 Ідентифікація та автентифікація. Криптографічні протоколи аутентифікації

(Автор: Марина Соловйова. Не редагувалось.)
(Версія від 19 січня 2017 р.)

Ідентифікація - це надання суб'єкту (об'єкту) індивідуального кода (наприклад, номера), тобто ідентифікатора, який відрізняється від всіх інших, а також перевірка ідентифікатора(все це не секретні дані).

Автентифікація - це перевірка достовірності суб'єкту по наданим ідентифікаторам та деякій додатковій інформації (наприклад, паролям, ключам) шляхом порівняння.

При контакті користувача, наприклад, з комп'ютерною мережею здійснюються наступні процедури:

- ідентифікація
- автентифікація
- авторизація

Принципи аутентифікації

1. По наданню деякої секретної інформації, відомої користувачеві (пароль, код).
2. По наданню деяких об'єктивних характеристик (мікросхема, магнітна стрічка).
3. По наданню індивідуальних біометричних характеристик (відбитків пальців, рисунку райдужної оболонки ока, тембру голосу).
4. По характеристикам роботи з апаратурою в реальному часі.
5. По відповідям в режимі діалогу.
6. За допомогою третьої сторони.

Криптографічні протоколи аутентифікації

1. Автентифікація за допомогою пароля (на прикладі аутентифікації з комп'ютерною системою – надалі будемо позначати як «КС»).

(a) *Парольна автентифікація з використанням односторонніх функцій*

Нехай h(x) – одностороння хеш-функція, що володіє сильною стійкістю до колізій.
Користувачі A_i мають ідентифікатори D_i та паролі p_i, i = $\overline{1,n}$.

i. Попередньо в КС формується та розміщується табличка
T = $\{D_i, H_i, i = \overline{1,n}\}$, де $H_i = h(p_i,D_i)$.
ii. (При контакті) $A_i : (p_i,D_i) \to$ КС.
iii. КС перевіряє: $?D_i \in T?$ (ідентифікація),
iv. $?h(p_i, D_i) = H_i? \longleftrightarrow ?H_i \in T?$ (автентифікація).
v. Якщо все виконується, то авторизація, інакше - відмова.

(b) *Паралельна автентифікація за допомогою симетричного шифрування стійких до атак на основі відкритого тексту (ВТ).*

Користувачі A_i мають ідентифікатори D_i та паролі p_i, $i = \overline{1,n}$.
Нехай E_k - алгоритм симетричного шифрування, стійкий до атак на основі ВТ.

i. Попередньо в КС формується та розміщується табличка
ii. T = $\{D_i, C_i, i = \overline{1,n}\}$, де $C_i = E_{p_i}(D_i)$.
iii. $A_i : (p_i,D_i) \to$ КС.
iv. КС перевіряє: $?D_i \in T?$ та $?E_{p_i}(D_i) = C_i?$
Якщо все виконується, то авторизація, інакше – відмова.

(c) *Парольна автентифікація з захистом від коротких паролів.*

i. модифікація в варіанті 1 з хеш-функцією h(x) - використання односторонніх хеш-функцій з секретним ключем (який відомий лише адмін-у КС).
ii. модифікація в варіанті 2: табличка T = $\{D_i, C_i, i = \overline{1,n}\}$ - використання секретного ключа k: $C_i = E_{p_i \oplus k}(D_i)$.
Перевірка аналогічна.

(d) *Парольна автентифікація зі змінним паролем.*

Користувачі A_i мають ідентифікатори D_i та паролі $p_i^{(0)}, i = \overline{1,n}$.
Наявна одностороння стійка до колізій хеш-функція h(x) (відкрита).

i. Кожен A_i обчислює ряд разових паролів:

$$p_i^{(0)}, p_i^{(1)} = h(p_i^{(0)}), p_i^{(2)} = h(p_i^{(1)}) = h^2(p_i^{(0)}) \vdots p_i^{(t)} = h^t(p_i^{(0)}) \text{ та } p_i^{(t)} \to \text{КС}, i = \overline{1,n}.$$

ii. КС формує табличку T = $\{D_i, p_i^{(t)}, i = \overline{1,n}\}$.
iii. (При контакті) $A_i : (D_i, p_i^{(t-1)}) \to$ КС.
iv. КС перевіряє: $?D_i \in T?$ та $?h(p_i^{(t-1)}) = p_i^{(t)}?$
Якщо все в виконується, то виконується авторизація і КС в табличці T змінює $(D_i, p_i^{(t)})$ на $(D_i, p_i^{(t-1)})$.
v. (При другому контакті) $A_i : (D_i, p_i^{(t-2)}) \to$ КС.
vi. КС перевіряє: $?D_i \in T?$ та $?h(p_i^{(t-2)}) = p_i^{(t-1)}?$

Якщо все виконується, то КС в табличці T змінює $(D_i, p_i^{(t-1)})$ на $(D_i, p_i^{(t-2)})$.
Примітка: Якщо всі разові паролі будуть вичерпані, потрібно згенерувати нові їх послідовності.
Але що робити при технічному збої? Зрозуміло, що повторювати пароль не можна. Тому при, наприклад, однократному збої на кроці 6): $A_i : (D_i, p_i^{(t-3)}) \to$ КС. Після чого КС перевіряє: $?D_i \in T?$ та $?h^2(p_i^{(t-3)}) = p_i^{(t-1)}?$ після чого алгоритм продовжує свою роботу.

2. Автентифікація за допомогою симетричних криптосистем.

   Користувачі A_i, $i = \overline{1,n}$ мають ідентифікатори D_i та K_{ij} - секретні ключі A_i та A_j зі спільною системою симетричного шифрування (E_k, D_k).

   (a) Ініціатор аутентифікації $A_i : D_i \to A_j$.

   (b) A_j генерує випадкове $M \to A_i$.

   (c) A_i шифрує на спільному ключі повідомлення: $E_{K_{ij}}(M) = C_{ij} \to A_j$.

   (d) A_j перевіряє: $D_{K_{ij}}(C_{ij}) = M$.

3. Автентифікація за допомогою асиметричних криптосистем (на прикладі RSA).

   Користувачі A_i, $i = \overline{1,n}$ мають відкриті (n_i, e_i) та закриті d_i ключі RSA.

   (a) За допомогою цифрового підпису (ЦП).

      i. A_i генерує випадкове M і підписує його, тобто:
      $S = M^{d_i} mod\ n_i, \Rightarrow (M, S) \to A_j$.

      ii. A_j перевіряє ЦП: $?S^{e_i} mod n_i = M?$

      iii. За допомогою шифрування.

4. Автентифікація за допомогою протоколу доказу без розголошення.