Криптография, Лекция № 6

13 октября 2014 г.

1 Шифрование с закрытым ключом (симметричное)

Схема:

$$x \longrightarrow S \longrightarrow R \longrightarrow x$$

S и R знают ключ d. На второй строчке есть еще A (Ева), который пытается что-то узнать об x. Он ничего не должен узнать об x, а точнее он может узнать только то, что он мог бы узнать без входа.

Формально:

Definition 1.
$d = D(1^n)$, D - генератор ключей, вероятностный полиномиальный алгоритм.
$m = E(x, d)$ - алгоритм шифрования, вероятностный полиномиальный алгоритм.
$y = D(m, d)$ - алгоритм дешифрования, вероятностный полиномиальный алгоритм.
Условине корректности: $Pr\{D(E(x, d), d) = x\} \simeq 1$, где $\simeq$ означает стремление быстрее любого полинома.
Условие надежности: $E(x, d)$ и $E(x', d)$ вычислительно не отличимы.

Любая пара протоколов, для которых это верно будет называться схемой шифрования с закрытым ключом.

Гаммирование (one-time pad): $E(x, d) = x \oplus D$, $D(m, d) = m \oplus d$, $|d| = |x|$. Выполнение условий корректности и надежности проверяется легко. Проблема в длине ключа. И в том, что схема одноразовая, ибо если зашифровать x и y, то станет известна побитовая сумма x и x'.

Гаммирование с генератором псевдо-случайных чисел: $E(x, d) = x \oplus G(d)$, $D(m, d) = m \oplus G(d)$. Здесь $|x| = poly(|d|)$. Но схема по-прежнему одноразовая. Чтобы сделать многоразовую схему можно вязть генератор отображающий n бит в $20n$.

Недостаток шифрования с закрытым ключом: нужен закрытый канал, для передачи ключа.

2 Шифрование с открытым ключом (асиметричное)

Есть два ключа: e - для шифрования и d - для дешифрования. e известнен A. R генерирует пару ключей e и d и публикует ключ e. И предлагает шифровать сообщения себе этим ключом.

Условие корректности: $Pr\{D(E(x,e),d) = x\} \simeq 1$.
Условие надежности: $(e, E(x,e))$ и $(e, E(x',e))$ вычислительно не отличимы.

Инструмент: одностороние перестановки с секретом (trapdoor one-way permutations). В одну сторону их вычислить легко, в другую - трудно, но легко с секретом.

Формально:

Definition 2.
4 функции:

- K - генератор номера функции и секрета
- S - выбор случайной точки 0.0
- F - вычисление значение функции
- B - при известном значении секрета вычисляет преобразования

Все эти функции полиномиальные, две из них обязательно вероятностные.

Theorem 1.
Если существует одностороняя перестановка с секретом, то существует односторонняя перестановка с секретом и трудным битом.

Remark 1.
Теорема доказывается аналогично теоремы с прошлого занятия (секрет останется тем же самым).

Примеры (предположительные):

1. Функция Рабина
   $x \mapsto x^2 (mod\, pq)$, где p, q - простные числа вида $4k+3$, x - квадратичный вычет.
   Открытый ключ - $p * q$, закрытый ключ - (p, q).
   Если секрет известен, то по $z = x^2$ можно восстановить x. А $x = t^2$. Поэтому $z^{\frac{p+1}{4}} = t^{p+1} \equiv t^2 \equiv x(mod\ p)$
   $z^{\frac{q+1}{4}} \equiv x(mod\ q)$. Из последних двух сравнений по китайской теореме об остатках можно найти x.

2. Функция RSA:
   $x \mapsto x^z (mod\ pq)$, где p, q - простые, $(z, \varphi(pq)) = 1$
   Секрет u берем из $z \cdot u = 1\ (mod\ \varphi(p,q))$
   $(x^z)^u = x^{x \cdot u} = x^{\varphi(pq) \cdot k+1} \equiv x \cdot 1^k = x\ (modpq)$

Оба примера основываются на том, что предположительно нельзя быстро раскладывать на простые множители.

Построение схемы шифрования с открытым ключом:
1 бит $b \in \{0, 1\}$. Пусть $q_\alpha(x)$ - одностороняя перестановка с секретом, $h_\alpha(x)$ - трудный бит для этой перестановки.

$$b \mapsto (g_{\alpha(x)}, h_\alpha(x) \oplus b)$$

Проверим условие надежности:
$(g_{\alpha(x)}, h_\alpha(x) \oplus b)$ - псевдо-случайная строка длины $n+1$ (ибо если h_α - трудный бит, то и $h_\alpha \oplus 1$ - трудный бит)
Если много битов:

$$b_1, \dots, b_k \mapsto (b_1 \oplus h_\alpha(x), b_1 \oplus h_\alpha(g_\alpha(x))), \dots, b_k \oplus h_\alpha(g_\alpha^{k-1}(x), g_\alpha^k(x))$$

Доказательство надежности похоже на доказательство вычислимой неотличимости в генераторах. Нужно идти с конца.