СОЗДАНИЕ СКРЫТОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ В БЕСПРОВОДНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Бродовская В.В, Филимонова А.В., Куржеевский И.В.
Научный руководитель: Куржеевский И.В.
Академия военно-морских сил им. П.С. Нахимова, Украина
E-mail: Violetta94@yandex.ru

Аннотация — В данной работе рассматривается создание скрытого канала передачи данных в беспроводных вычислительных сетях на основе цифровой подписи Онга-Шнорра-Шамира.

1. Введение

В вычислительных сетях возможно создание скрытого канал передачи данных при использовании алгоритмов электронной цифровой подписи (ЭЦП). Скрытый канал — непредусмотренный разработчиком коммуникационный канал, по которому могут быть переданы сообщения. Впервые концепцию создания скрытого канала предложил Г. Симмонс [1].

2. Основная часть

Для организации скрытого канала передачи данных, абонент А создает несекретное электронное цифровое письмо, которое подписывает своей ЭЦП. Рассмотрим алгоритм создания скрытого канала передачи данных на основе ЭЦП Онга-Шнорра-Шамира, согласно которого:

— необходимо сгенерировать простое число p.
p:=20965_57522_55599_48381_65640_12682_89294_80366_27757_04125_85321;

— необходимо сгенерировать простое число *q*.
q:=524_13938_06389_98709_54141_00317_07232_37009_15693_92603_14633;

— перемножить простые числа *p* и *q*.
$n = p \times q$;
n=109_88883_61346_53270_11519_55309_94082_21433_82869_49067_30074_98751_09077_70284_21779_75910_88737_35685_76934_77622_54173_02193;

— абонентом А выбрать случайное число k НОД $(k, n) = 1$, в качестве секретного ключа, и безопасным образом передает абоненту В.
k=101_38471_35900_09972_41845_07521_12418_54002_29300_24391_39080_52433_88030_17857_85033_54028_57616_38594_50522_62960_45698_08558.

— согласно алгоритму вычислить открытый ключ ЭЦП. $h = -k^{-2} (\mathrm{mod}\, n)$ и получить
h=106_87870_09061_52833_61191_83933_52053_17318_65530_00604_35905_82962_46703_49048_65535_67486_08392_19351_49936_28845_03235_29065;

— найти M — хеш-значение документа
M:=1382_84847_09165_00511_11918_70517_30116_45583_99521_29616;

— скрытое сообщение, (например: «Явка провалена Петров предатель, связь по запасному каналу».), зашифровывать в виде числа *r*.
r=33341_20134_17181_60301_13061_50134_17062_01816_03341_71806_05012_00613_28341_90333;

— вычислить первую часть ЭЦП, согласно алгоритму

$$S_1 = \frac{1}{2}\left(\frac{M}{r} + r\right) \mathrm{mod}\, n \qquad (1)$$

и получить
S_1=108_26089_00102_01367_24697_41536_81577_31147_90246_28873_59350_68774_71930_68760_78681_63442_25996_57098_18051_47207_25418_03135;

— вычисляем вторую часть ЭЦП, согласно алгоритму

$$S_2 = \frac{k}{2}\left(\frac{M}{r} - r\right) \mathrm{mod}\, n \qquad (2)$$

и получить
S_2=23_04330_44609_99093_36824_22900_31352_18910_36684_11661_84201_71445_01324_73699_70302_73771_10316_37970_47167_31875_92211_25785;

— проверку подлинности ЭЦП осуществить по формуле $M' = (S_1^2 + hS_2^2) \mathrm{mod}\, n$ (проверяющая сторона С может убедиться в том, что подпись подлинная, а передаваемая ЭЦП и подпись к нему в явном виде скрытой информации не содержит);

— получить скрытую информацию можно по следующей формуле

$$R = \frac{M}{S_1 + \frac{S_2}{k}}. \qquad (3)$$

Докажем, что эти вычисления позволяют извлечь скрытую информацию. Для этого, подставив в формулу (3), S_1 из (1) и S_2 из (2), получим

$$\frac{M}{\frac{1}{2}\left(\frac{M}{r} + r\right) + \frac{\frac{k}{2}\left(\frac{M}{r} - r\right)}{k}} = \frac{M}{\frac{1}{2}\left(\frac{M}{r} + r + \frac{M}{r} - r\right)} =$$

$$= \frac{M}{\frac{1}{2} \times \frac{2M}{r}} = r.$$

3. Заключение

В качестве борьбы со скрытым каналам передачи данных, авторы предлагают использовать в алгоритме Онга-Шнорра-Шамира не случайное r, а числа сгенерированные по алгоритму Нидхема-Шрёдера [2].

4. Список литературы

[1] Simmons G.J. The Prisoner`s problem and the subliminal channel // Proc. of CTYPTO `83. — New York: Plenum Press, 1984. — P. 51 — 67.
[2] Needham R.M. Using encryption for authentication in large networks of computers / R.M. Needham, M.D. Schroeder // Commun. ACM. — 1978. — T. 21, № 12. — P. 993 — 999.

CREATING HIDDEN DATA CHANNEL IN A WIRLESS COMPUTING NETWORKS

Brodovska V.V., Filimonova A.V., Kurzheievskyi I.V.
Scientific adviser: Kurzheievskyi I.V.
Naval Academy named after P.S. Nakhimov, Ukraine

Abstract — The questions of the creation of the covert channel data transmission in wireless computing networks, based on a digital signature Ong-Schnoor-Shamira, are considered. The hidden channel is the unsolicited developer communication channel, which allows sending through the messages.