Ассоциация РусКрипто

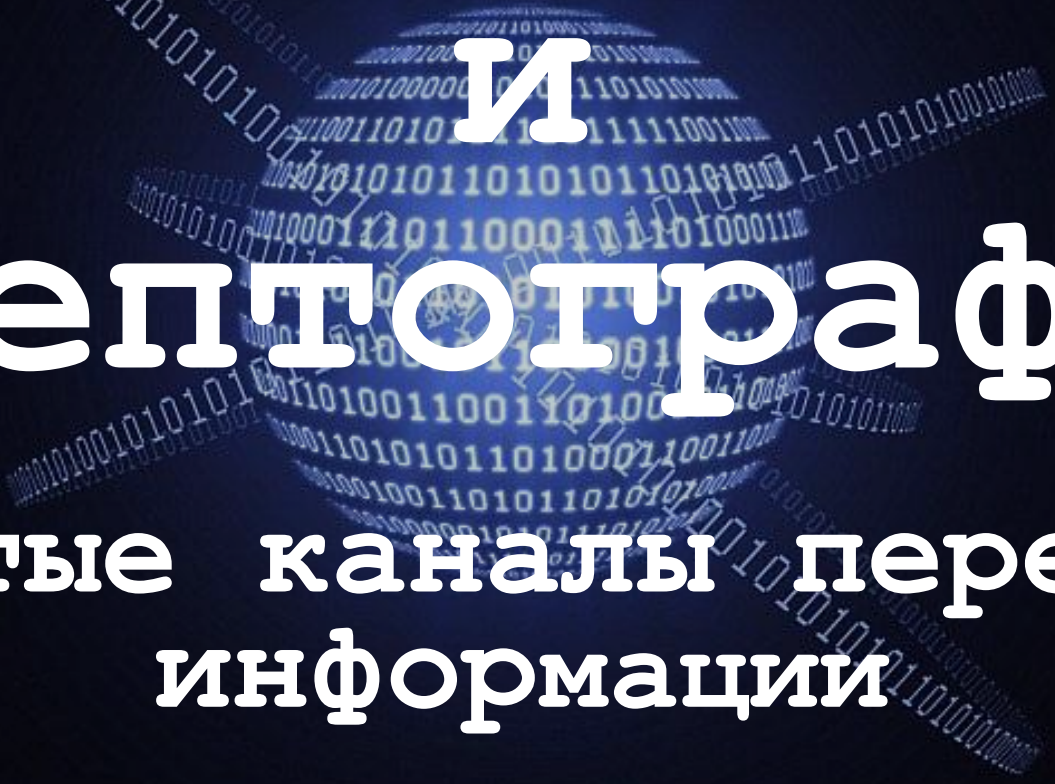
РусКрипто 2017

Ассоциация РусКрипто

РусКрипто 2017

Криптография и клептография

Скрытые каналы передачи информации



Ассоциация РусКрипто

Гражданская криптография

Ассоциация РусКрипто

Гражданская криптография

Ассоциация РусКрипто

Крипто-войны

Ассоциация РусКрипто

Крипто-войны

Ассоциация РусКрипто

Крипто-войны

Ассоциация РусКрипто

Рост терроризма

Ассоциация РусКрипто

Число жертв терактов

Ассоциация
РусКрипто

Ассоциация РусКрипто

Investigatory Powers Act

Ассоциация
РусКрипто

Ассоциация РусКрипто

Крипто-войны

Ассоциация РусКрипто

Криптосистемы со встроенными лазейками

Clipper chip

Dual_EC_DRBG

NIST Special Publication 800-90A


NIST Special Publication 800-90

Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)

Elaine Barker
John Kelsey

Computer Security Division
Information Technology Laboratory

COMPUTER SECURITY

March 2007

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

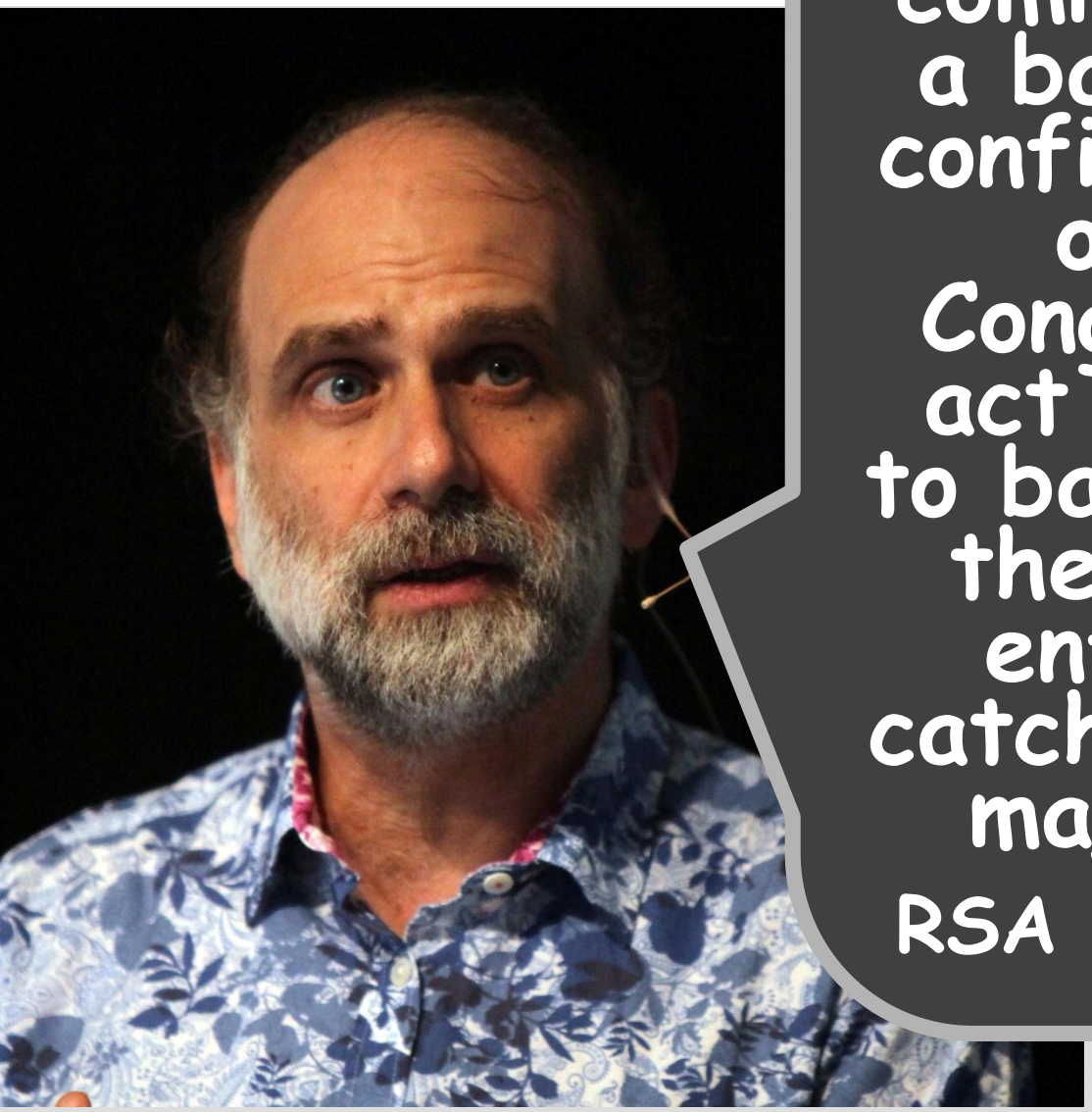
National Institute of Standards and Technology
William Jeffrey, Director

Ассоциация РусКрипто

Крипто-войны

Ассоциация РусКрипто

Крип

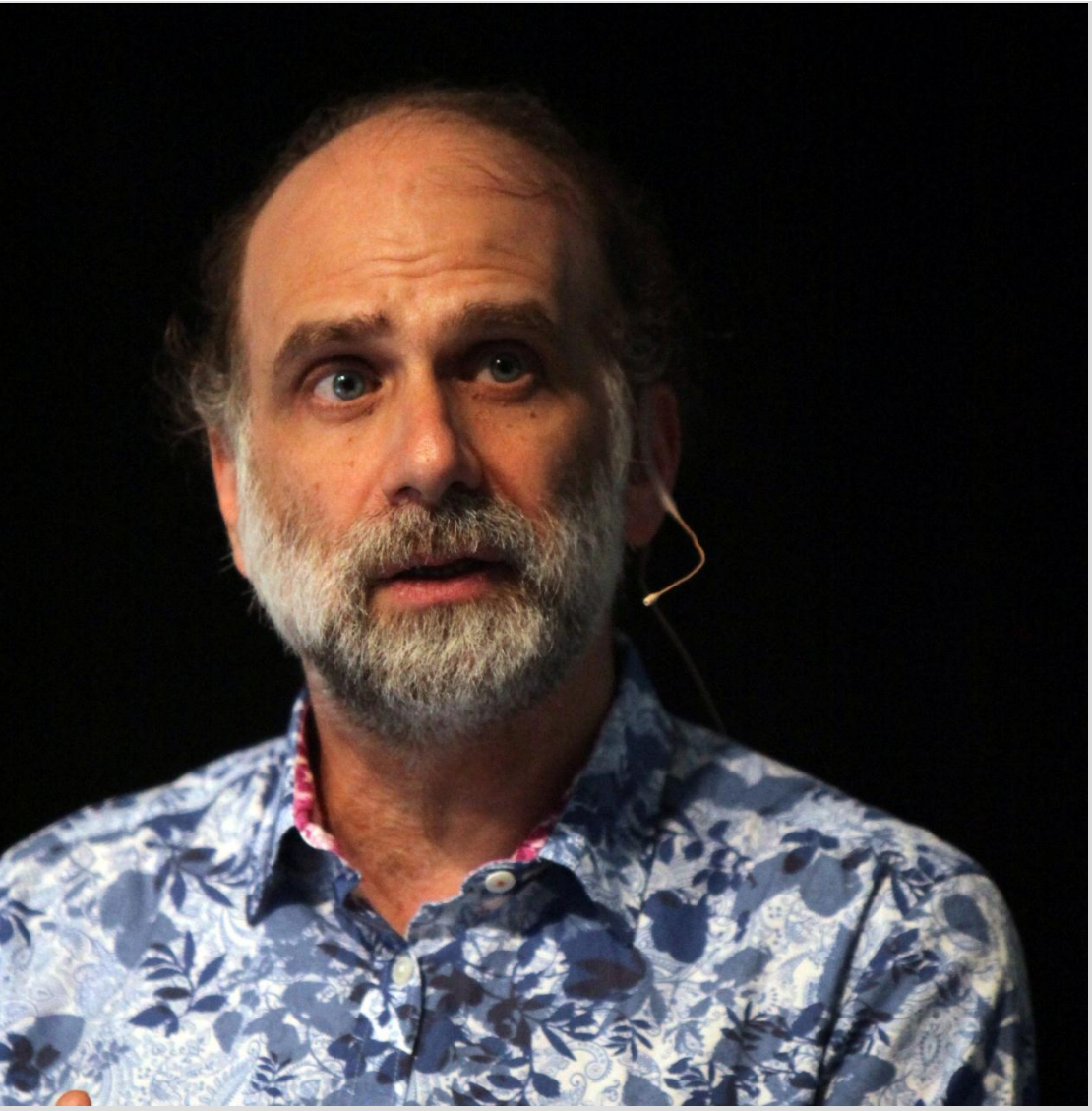


Backdoors to break into encrypted communications are a bad idea from a confidentiality point of view, but Congress needs to act to decide how to balance that with the needs of law enforcement to catch terrorists and major criminals.

RSA Conference 2016.

Ассоциация РусКрипто

Крипто-войны



Ассоциация
РусКрипто

Ассоциация
РусКрипто

Скрытые каналы передачи информации

Ассоциация РусКрипто

Скрытые каналы передачи информации

G. J. Simmons

The Prisoners' Problem and the Subliminal Channel,

Proceedings of Crypto'83, Plenum Press, 1984

Ассоциация РусКрипто

Скрытые каналы передачи информации

Основные вопросы, возникающие при пользовании криптографическими «черными ящиками»:

1. Предоставляет ли алгоритм недокументированные возможности и, в частности, содержит ли алгоритм незаявленные включения, позволяющие реализовать эти возможности?

Скрытые каналы передачи информации

2. Допускает ли он утечку секретной информации?

3. Возникает ли риск для пользователя, в случае успешного реверс-инженеринга данного алгоритма третьей стороной?

Ассоциация РусКрипто

Скрытые каналы передачи информации

- Канал называется *нелегальным (нестандартным)* – (hidden, covert), если он специально не проектировался и изначально не предполагался для передачи информации в электронной системе обработки данных.

Ассоциация РусКрипто

Скрытые каналы передачи информации

- На практике, нелегальные каналы утечки информации трактуются шире и рассматриваются не только нестандартные каналы передачи информации, но и нестандартные способы передачи информации по легальным каналам.

Ассоциация РусКрипто

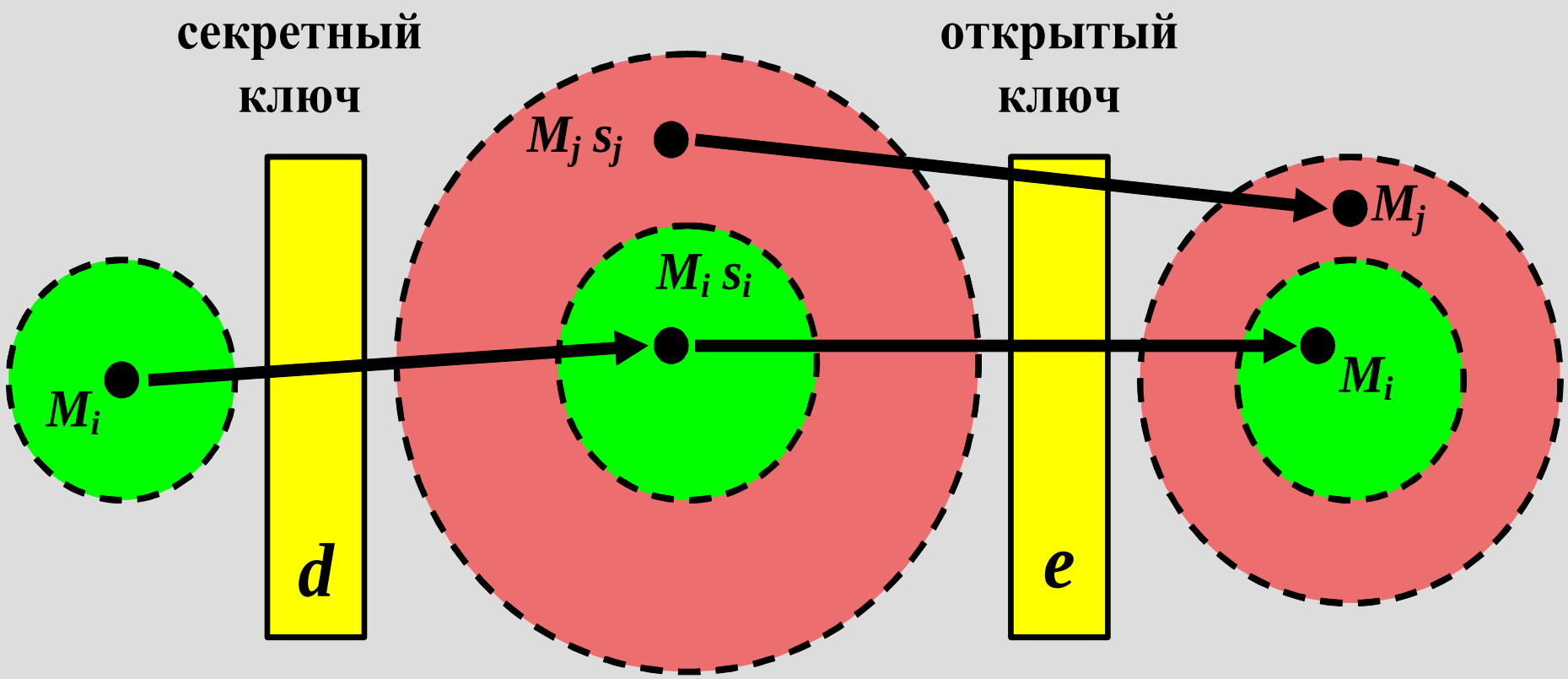
Скрытые каналы передачи информации

- Нестандартный канал называется *скрытым* (subliminal), если воспользоваться им может только обладатель соответствующей информации (ключа).

Ассоциация РусКрипто

Скрытые каналы передачи информации

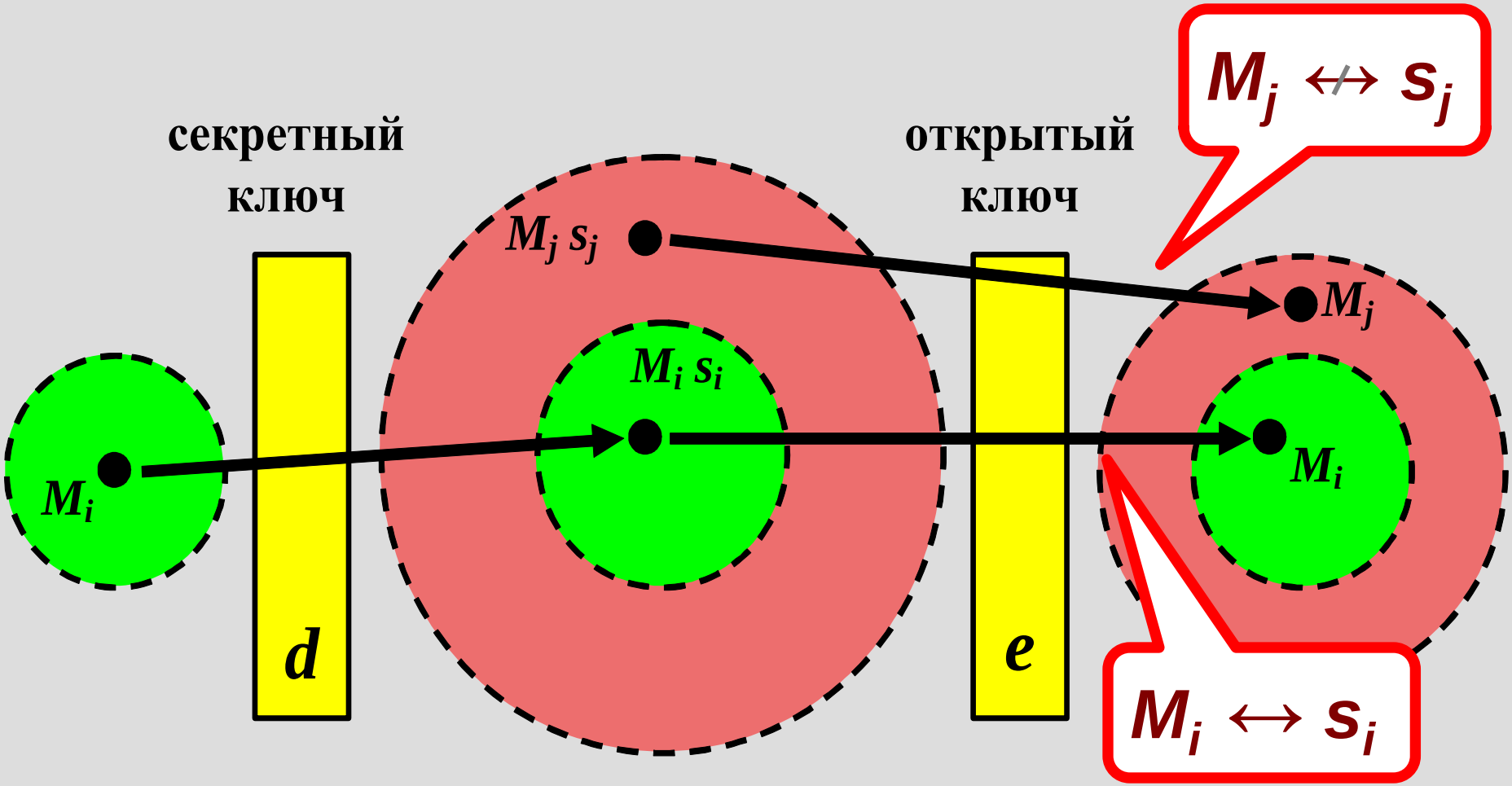
Gustavus J. Simmons



Ассоциация РусКрипто

Скрытые каналы передачи информации

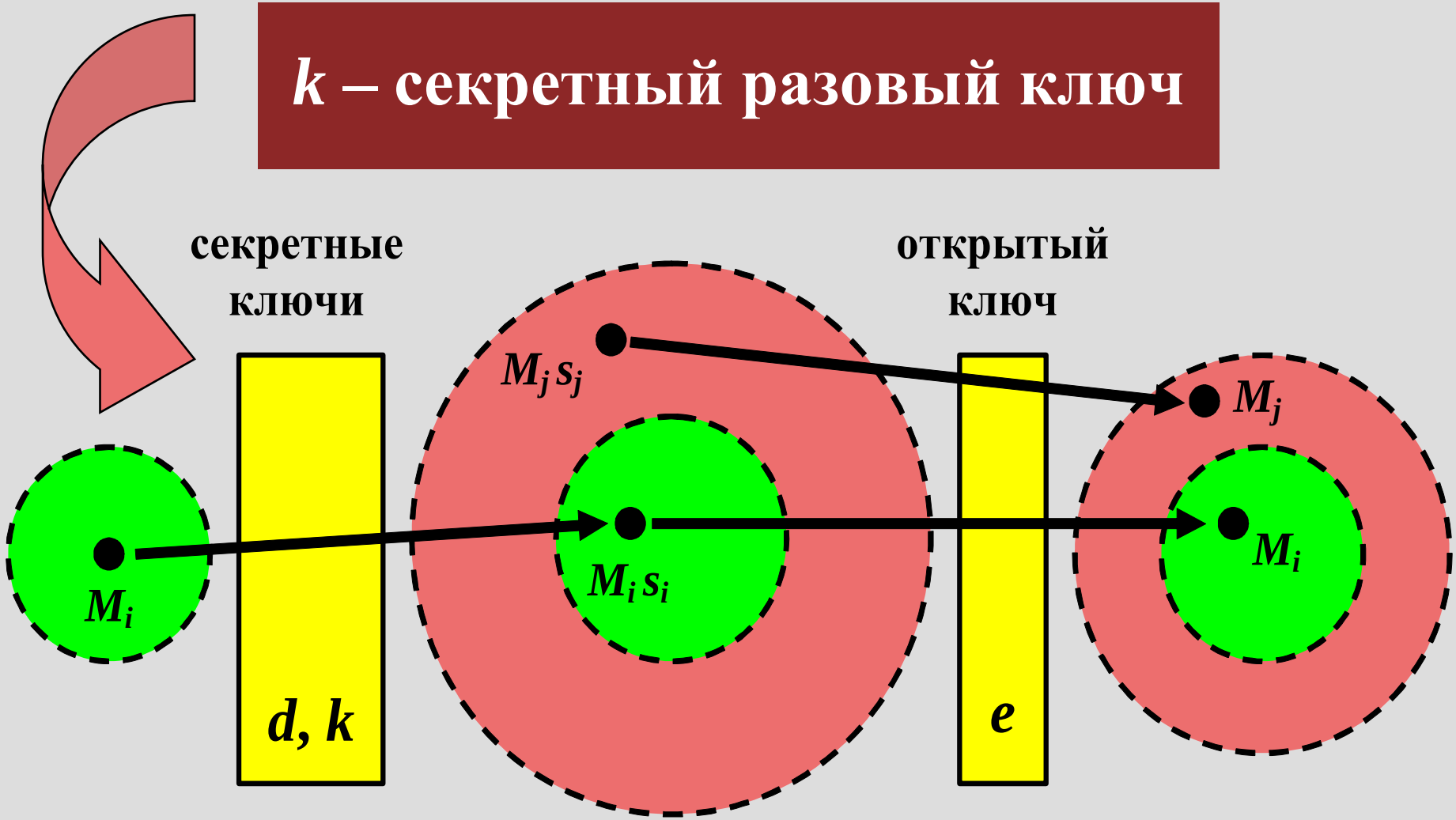
Gustavus J. Simmons



Ассоциация РусКрипто

e – открытый ключ
d – секретный ключ
} – долговременные ключи

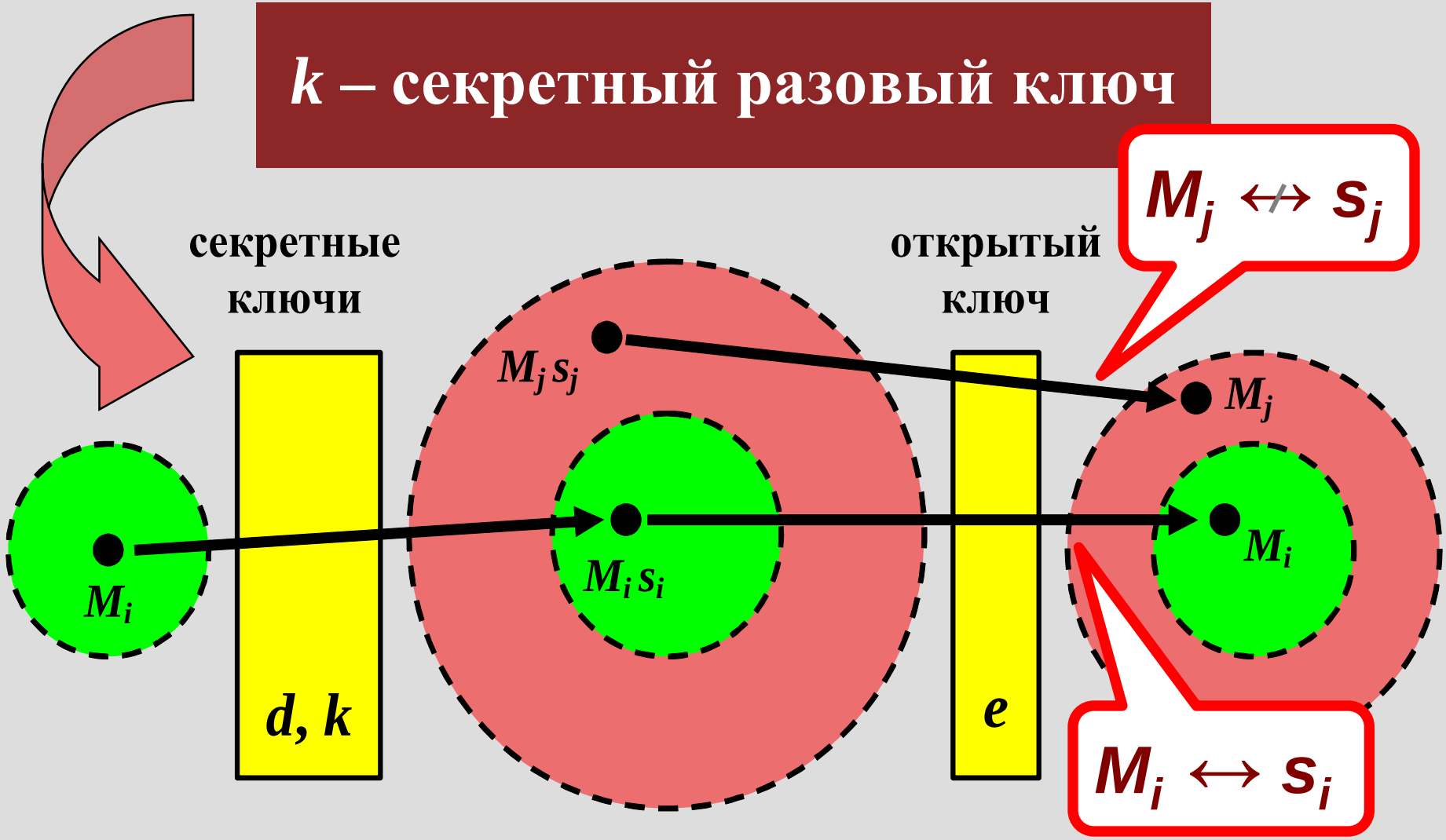
k – секретный разовый ключ



Ассоциация РусКрипто

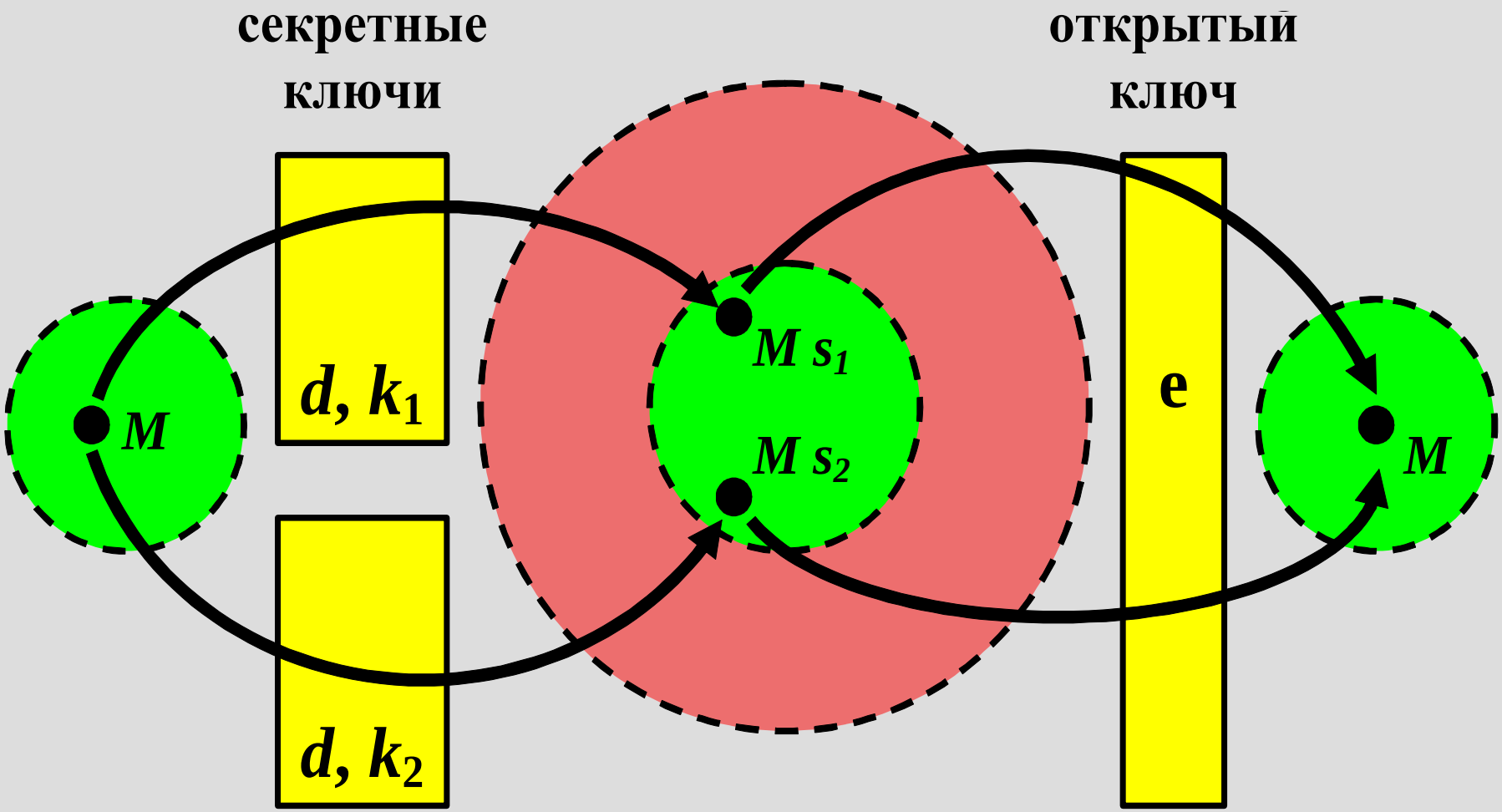
e – открытый ключ
d – секретный ключ
} – долговременные ключи

k – секретный разовый ключ



Ассоциация РусКрипто

Передача 1 бита информации:



Скрытые каналы передачи информации в реальных системах

Ассоциация РусКрипто

Алгоритм DSA

p – простое в диапазоне 512-1024 бит,

q – простое 160 бит, $q \mid (p-1)$;

$$\forall h: \quad g = h^{\left(\frac{p-1}{q}\right)} \bmod p;$$

$$\forall d < q: \quad e = g^{d} \bmod p;$$

Открытый ключ: (p, q, g, e).

Секретный ключ: d.

Ассоциация РусКрипто

Алгоритм DSA
Выработка подписи:

***M* – сообщение,**

***k* < *q* – *случайное* – <u>секретный разовый ключ</u>**

<u>Подпись</u>: (*M*, *r*, *s*)

$$r = \left(g^{k} \bmod p \right) \bmod q;$$

$$s = \left(k^{-1} \left(H(M) + dr \right) \right) \bmod q$$

Ассоциация РусКрипто

Алгоритм DSA
Проверка подписи:

Подпись (M, r, s)

$$w = s^{-1} \bmod q$$

$$u_1 = \left(H(M) \times w\right) \bmod q$$

$$u_2 = rw \bmod q$$

$$v = \left(g^{u_1} \times e^{u_2} \bmod p\right) \bmod q$$

$$?$$

$$v = r$$

Ассоциация РусКрипто

Встраивание нелегального сообщения m:

Выбираем «случайное» число $k = m$

$$r = \left(g^k \bmod p\right) \bmod q; \quad s = \left(k^{-1}\left(H(M) + dr\right)\right) \bmod q$$

Подпись: (M, r, s)

Получение нелегального сообщения при известном d :

$$m = k = \left(s^{-1}\left(H(M) + dr\right)\right) \bmod q$$

Криптосистемы с лазейками

Алгоритм DSA входит в состав американского стандарта на цифровую подпись FIPS 186-1. Канал в этом алгоритме, позволяющий скрытно передавать информацию, существует *изначально* и обусловлен структурой самого алгоритма.

Встроенные каналы утечки информации (лазейки)

Криптосистемы со встроенными лазейками

Определим понятие *клептография*, как теорию построения информационных систем, содержащих безопасные и скрытые каналы утечки секретной информации.

Криптосистемы со встроенными лазейками

Adam Young, Moti Yung, "Kleptography: Using Cryptography Against Cryptography," Eurocrypt'97, LNCS 1233, pp. 62-74, 1997.

Криптосистемы со встроенными лазейками

При анализе работы клептографических систем следует выделить следующих трех участников:

Ассоциация РусКрипто

Криптосистемы со встроенными лазейками

- *Разработчик*: обладает информацией о лазейке, владеет секретным ключом к лазейке, не владеет секретным ключом пользователя.

Ассоциация РусКрипто

Криптосистемы со встроенными лазейками

- *Пользователь*: владеет секретным ключом пользователя, в случае успешного реверс-инженеринга обладает информацией о лазейке, но не владеет ее секретным ключом.

Ассоциация РусКрипто

Криптосистемы со встроенными лазейками

- ***Злоумышленник***: в случае успешного реверс-инженеринга обладает информацией о лазейке, но не владеет ее секретным ключом, а также секретным ключом пользователя.

Ассоциация РусКрипто

Криптосистемы со встроенными лазейками

- *Шифр с лазейкой* (backdoor) – это шифр, алгоритм которого содержит некоторую скрытую структуру (лазейку), обеспечивающую существование скрытого канала передачи информации; знание этой структуры позволяет получить секретную информацию (например, о секретном ключе)

Ассоциация РусКрипто

Криптосистемы со встроенными лазейками

- *Шифр с лазейкой* (trapdoor) – это шифр, алгоритм которого содержит некоторую секретную информацию (лазейку), обеспечивающую существование определенного способа передачи информации; знание этой структуры позволяет получить секретную информацию (например, о секретном ключе).

Без знания лазейки шифр кажется надежным.

Ассоциация РусКрипто

Криптосистемы со встроенными лазейками

Одним из наиболее важных типов лазеек, встраиваемых в криптографические алгоритмы является так называемый *SETUP-механизм*.

SETUP – Secretly Embedded Trapdoor with Universal Protection – секретно встроенная лазейка с универсальной защитой.

Ассоциация РусКрипто

Криптосистемы со встроенными лазейками

SETUP-механизм ***видоизменяет*** заданный криптографический алгоритм таким образом, что позволяет производителю криптосистемы получать секретную информацию пользователя (чаще всего информацию о его секретных ключах).

Встраивание лазеек в асимметричные криптоалгоритмы

Ассоциация РусКрипто

Протокол Диффи-Хеллмана

- **a – *случайное* число, выбираемое пользователем A – секретный «разовый ключ» пользователя A;**
- **b – *случайное* число, выбираемое пользователем B – секретный «разовый ключ» пользователя B.**

***Обмен информацией*:**

A: $y_A = g^a \rightarrow$ **B** **B:** $y_B = g^b \rightarrow$ **A**

***Вычисления*:**

A: $(y_B)^a = (g^b)^a = g^{ab} = K$ **B:** $(y_A)^b = (g^a)^b = g^{ab} = K$

Ассоциация РусКрипто

Протокол DH_SETUP

Клептосистема, встроенная пользователю A:

$h=g^{\delta}$, δ – секретно и известно только разработчику.

- **a_1 – случайное число, выбираемое пользователем A, его секретный разовый ключ для первого сеанса связи.**

В канал идет $y_1= g^{a}1 \rightarrow$ B.

Ассоциация РусКрипто

Протокол DH_SETUP

Для второго сеанса связи клептосистема вырабатывает «секретный» разовый ключ $a_2 = h^{a_1} + H(y_1)$ $(= g^{\delta a_1} + H(y_1)$ – псевдослучайное число.

В канал идет $y_2 = g^{a_2} \rightarrow$ B.

и т.д. …

Ассоциация РусКрипто

Протокол DH_SETUP

…

Для n-го сеанса связи

$a_n = h^{a_{n-1}} + H(y_{n-1})(= g^{\delta a_{n-1}} + H(y_{n-1}).$

В канал идет $y_n = g^{a_n} \rightarrow$ B.

Получение a_n:

$$a_n = (y_{n-1})^{\delta} + H(y_{n-1}) = g^{\delta a_{n-1}} + H(y_{n-1}).$$

Ассоциация РусКрипто

«Криптостойкость» протокола DH_SETUP

Протокол имеет скрытый канал утечки информации, который является безопасным. Протокол предоставляет исключительные права разработчику. Без знания величины δ, которая известна только разработчику, задача определения секретных разовых ключей a_n сведется к решению задачи дискретного логарифмирования.

Встраивание лазеек в симметричные алгоритмы шифрования

Ассоциация РусКрипто

Криптосистемы со встроенными лазейками

Mathematical Backdoors in Symmetric Encryption Systems*

Proposal for a Backdoored AES-like Block Cipher

Arnaud Bannier and Eric Filiol

Operational Cryptology and Virology Lab, ESIEA,
38 rue des Drs Calmette et Guérin, 53000 Laval, France,
{bannier, filiol}@esiea.fr

Ассоциация РусКрипто

Выводы

Ассоциация РусКрипто

Криптосистемы со встроенными лазейками

- Встроенный SETUP-механизм лазейки полностью компрометирует рассматриваемые криптосистемы по отношению к ее разработчику. Особенную опасность представляют SETUP-механизмы для smart-карт, т.к. генерация ключей в них всегда происходит без участия пользователя.

Ассоциация РусКрипто

Криптосистемы со встроенными лазейками

- Многие разработчики криптографических протоколов считают, хорошим правилом встраивание датчиков случайных чисел внутрь самих протоколов. Но если устройство выбирает «случайные числа» самостоятельно, то разработчику криптосистемы не составляет большого труда организовать скрытый канал.

Ассоциация РусКрипто

Общие рекомендации

Ассоциация РусКрипто

Общие рекомендации

1. Перед использованием криптографического примитива, его структура должна быть тщательно изучена и оценена.

   Нельзя безоговорочно доверять аппаратным компонентам с заданной спецификацией (необходима проверка реализации на соответствие спецификации, а также изучение самой спецификации). Даже программные реализации могут быть опасны, особенно, если исходных код и документация разработчика недоступны для проверки.

Ассоциация РусКрипто

Общие рекомендации

2. Прохождение тестов по формальным критериям не гарантирует отсутствия скрытых лазеек. В частности, нельзя принимать решение о доверии лишь на основании обширного статистического исследования.

   По-видимому, для любого фиксированного набора критериев можно построить криптосистему с лазейкой, которая, тем не менее, будет удовлетворять этим критериям.

Ассоциация РусКрипто

Общие рекомендации

3. Хорошую защиту от наличия скрытых лазеек в криптоалгоритмах дает композиция (каскадирование) криптопреобразований, имеющих происхождение из различных источников.

Ассоциация РусКрипто

Общие рекомендации

4. **Важен контроль за случайностью. Совершенно необходимо, чтобы алгоритмы выработки случайных величин, используемых в криптографических примитивах, были открыты для пользователя.**

   Если имеется программное обеспечение для выработки ключей – оно должно быть абсолютно надежным и доверенным. Хорошим выходом будет возможность использовать посторонний источник случайных чисел.

Ассоциация РусКрипто

Общие рекомендации

5. Лучше если источник случайности, генератор ключей и алгоритм, использующий их – три раздельных компоненты. При этом должна быть исключена возможность их обхода, сами они – из надежного источника, а каналы, связывающие их, не допускают утечку информации.

Ассоциация
РусКрипто