О протоколе установления защищенного соединения с функциональным ключевым носителем

Алексеев Е.К.
Ошкин И.Б., Попов В.О., Смышляев С.В.

КРИПТО ПРО

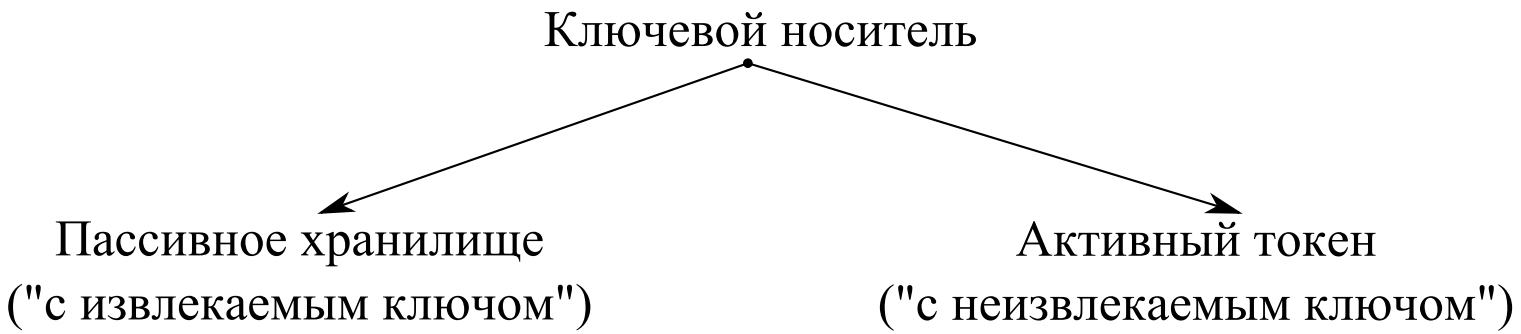
Безопасное хранение криптографических ключей

Задача безопасного хранения и использования криптографических ключей является одной из наиболее важных для защиты информации

Варианты решения

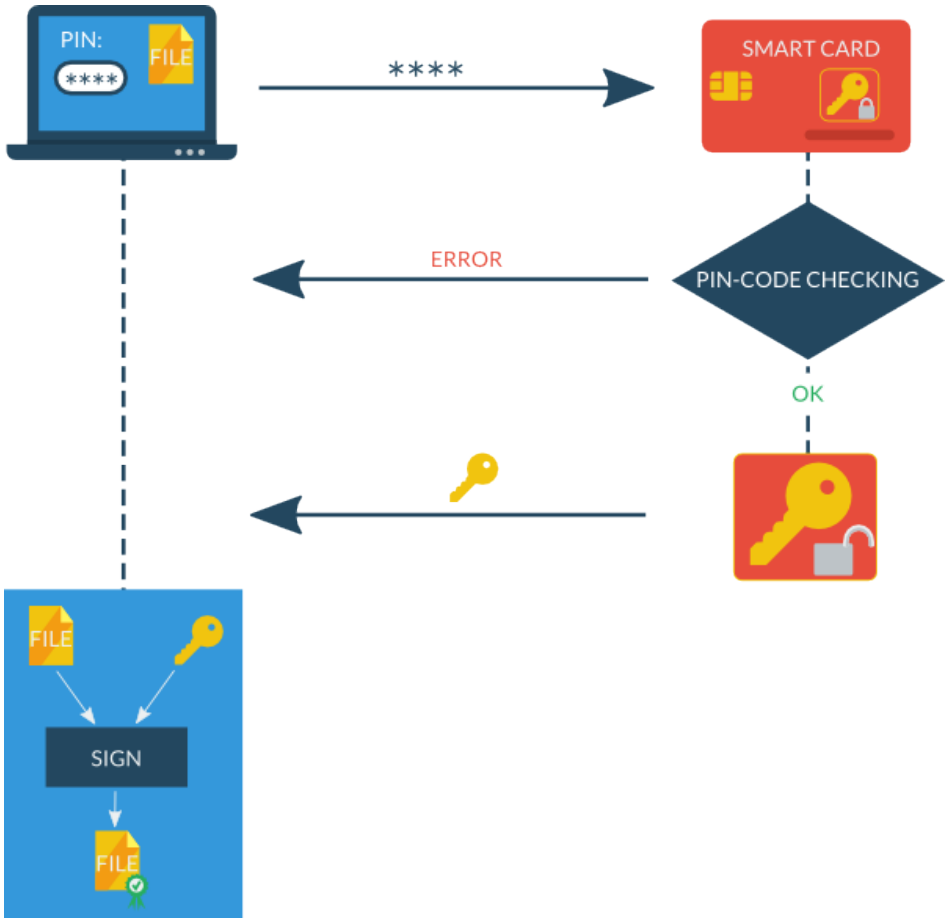
1) Запомнить ключ
2) Записать ключ на флэшку
3) Использовать специальный ключевой носитель
4) ...

Основные виды ключевых носителей



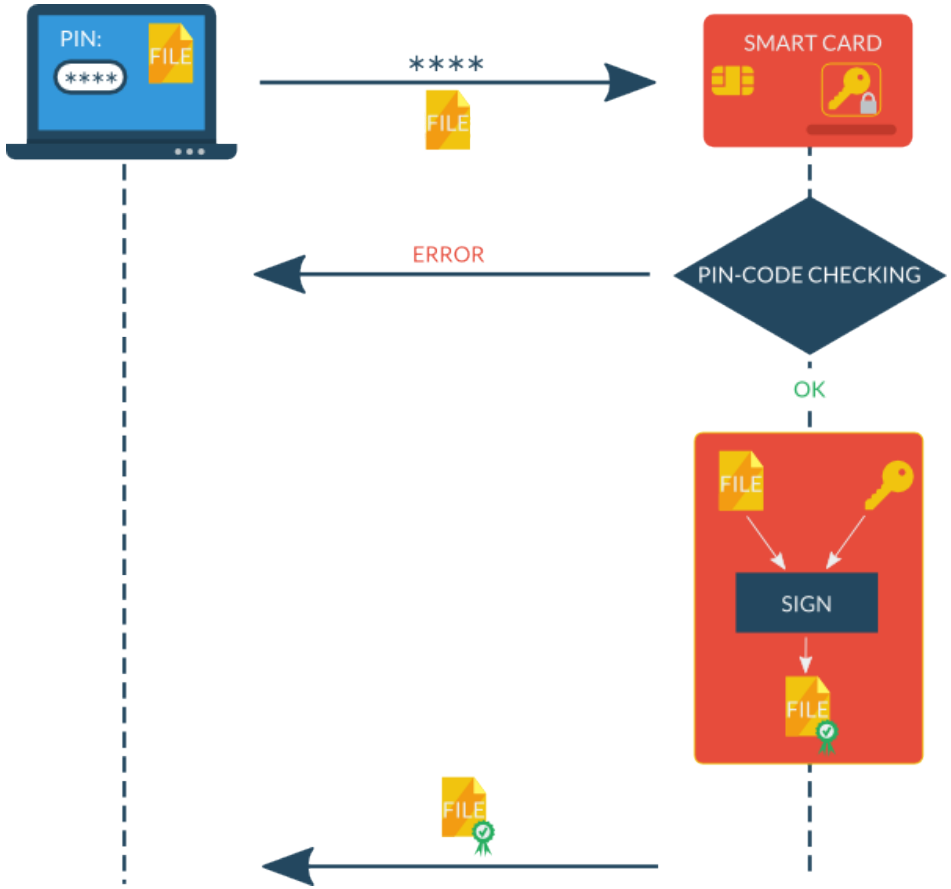
КРИПТО ПРО

Пассивное хранилище



КРИПТО ПРО

Активный токен



Основные виды ключевых носителей

Ключевой носитель

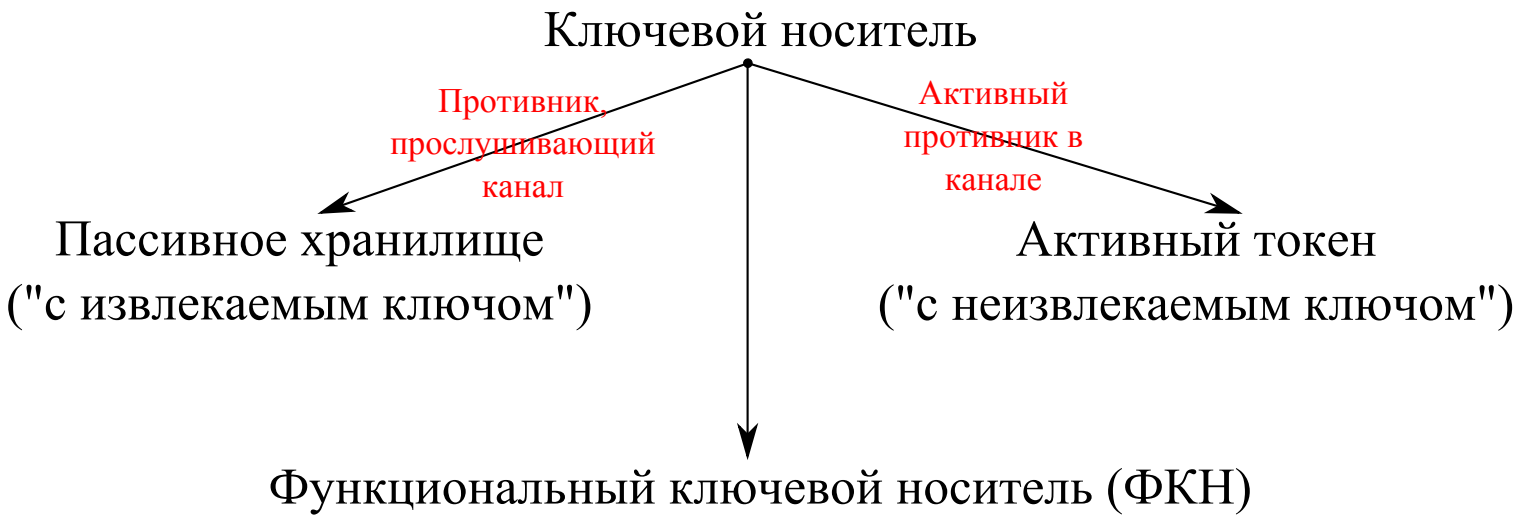
Противник, прослушивающий канал

Активный противник в канале

Пассивное хранилище ("с извлекаемым ключом")

Активный токен ("с неизвлекаемым ключом")

Основные виды ключевых носителей



КРИПТО ПРО

Основная цель

Ключевой носитель должен быть стойким по отношению к активному противнику в канале связи токен-машина

Основная идея

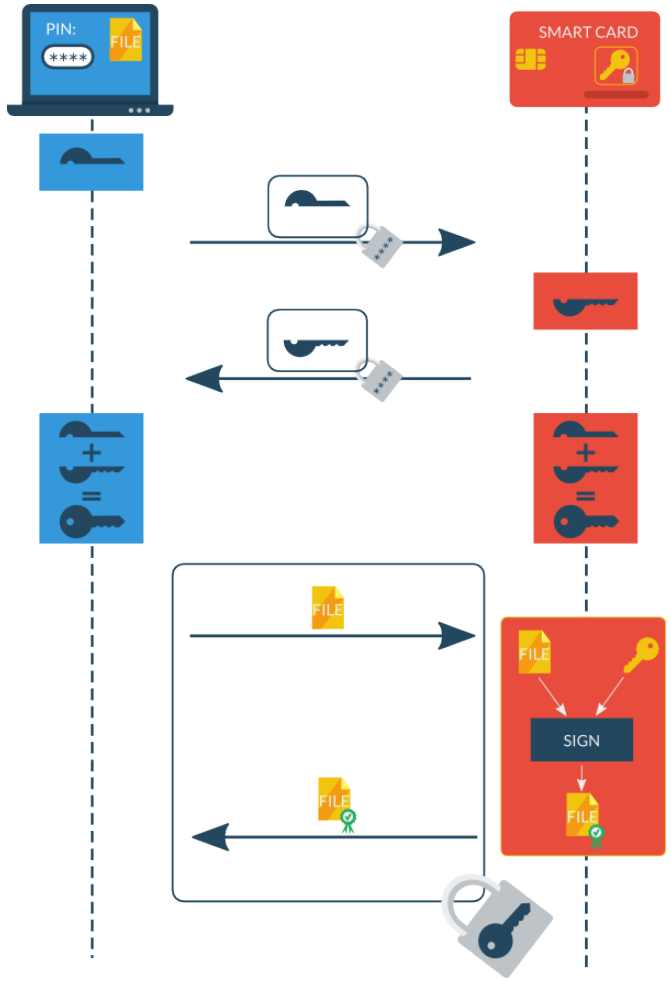
Данные, передаваемые для формирования защищенного канала, защищаются с помощью пароля на токен

Основное дополнительное к стандартным требование

Активный противник в канале не должен иметь возможность получить критерий для бесконтрольного угадывания пароля (так называемого ”offline-перебора”)

КРИПТО ПРО

Общая схема взаимодействия



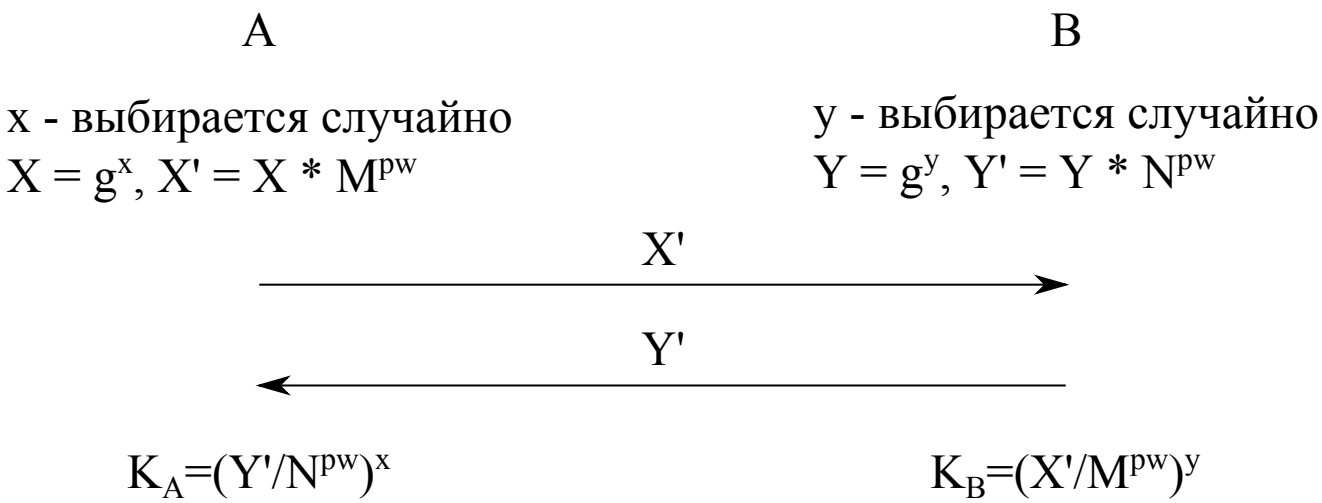
КРИПТО ПРО

Легко ли построить такой протокол?

КРИПТО ПРО

Пример 1: Как порождать сеансовый ключ?

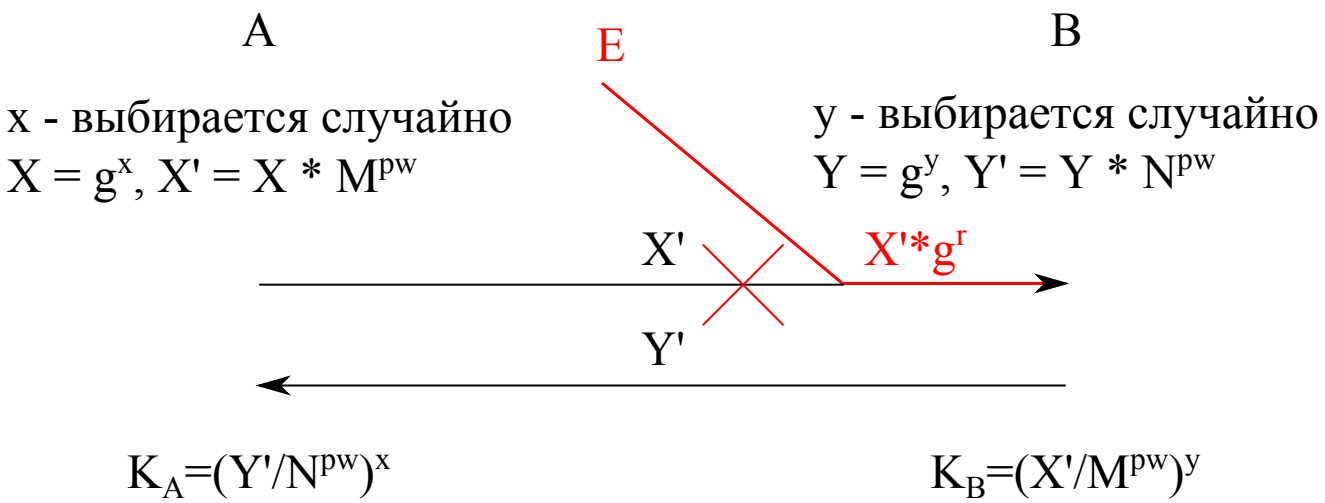
Пароль используется в качестве ”гаммы” при защите эфемерных ключей Диффи-Хеллмана. Сеансовый ключ не зависит от пароля. Здесь: $G = \langle g \rangle = \langle M \rangle = \langle N \rangle$.



КРИПТО ПРО

Пример 1: Как порождать сеансовый ключ?

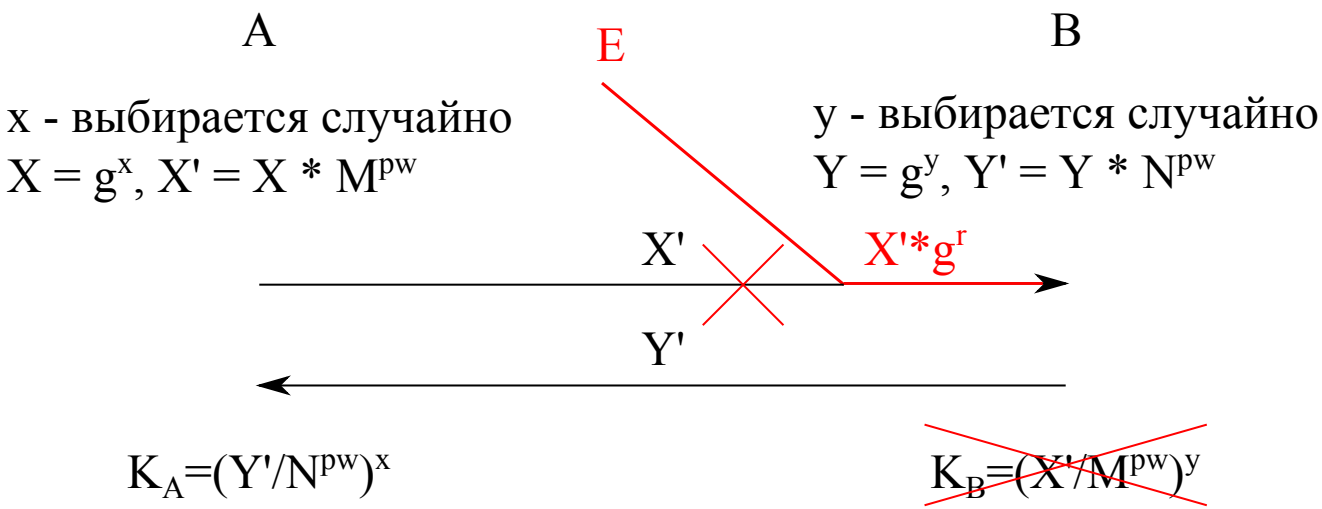
Пароль используется в качестве ”гаммы” при защите эфемерных ключей Диффи-Хеллмана. Сеансовый ключ не зависит от пароля. Здесь: $G = \langle g \rangle = \langle M \rangle = \langle N \rangle$.



КРИПТО ПРО

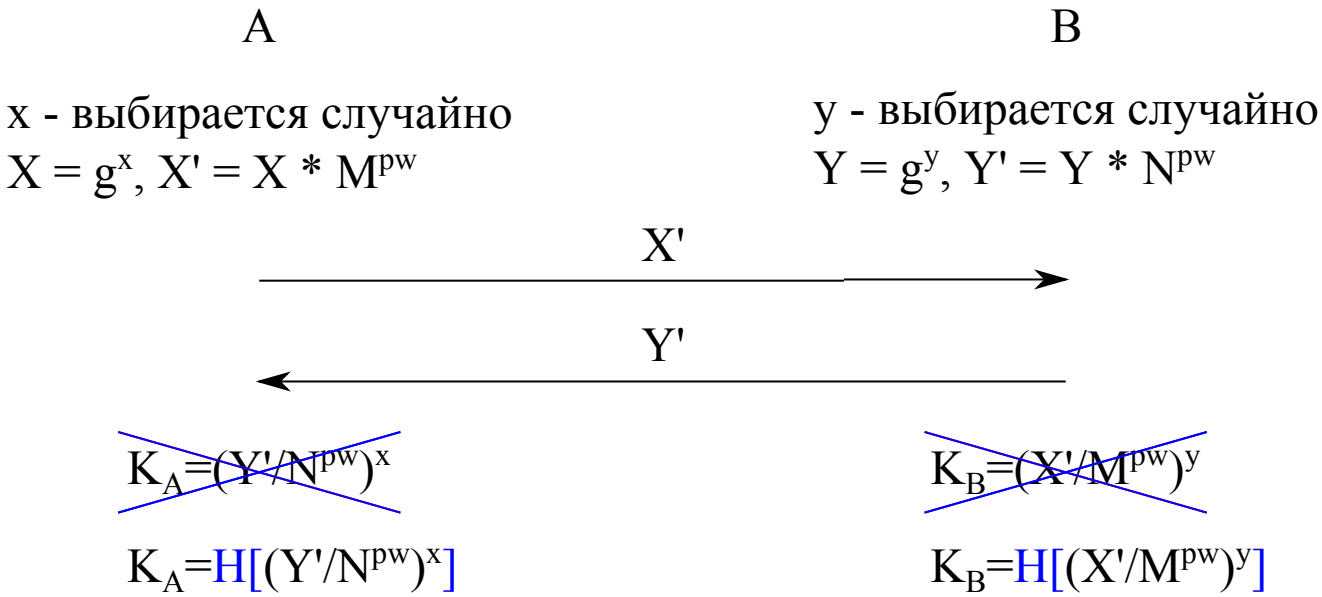
Пример 1: Как порождать сеансовый ключ?

Пароль используется в качестве ”гаммы” при защите эфемерных ключей Диффи-Хеллмана. Сеансовый ключ не зависит от пароля. Здесь: $G = \langle g \rangle = \langle M \rangle = \langle N \rangle$.



Пример 1: Как порождать сеансовый ключ?

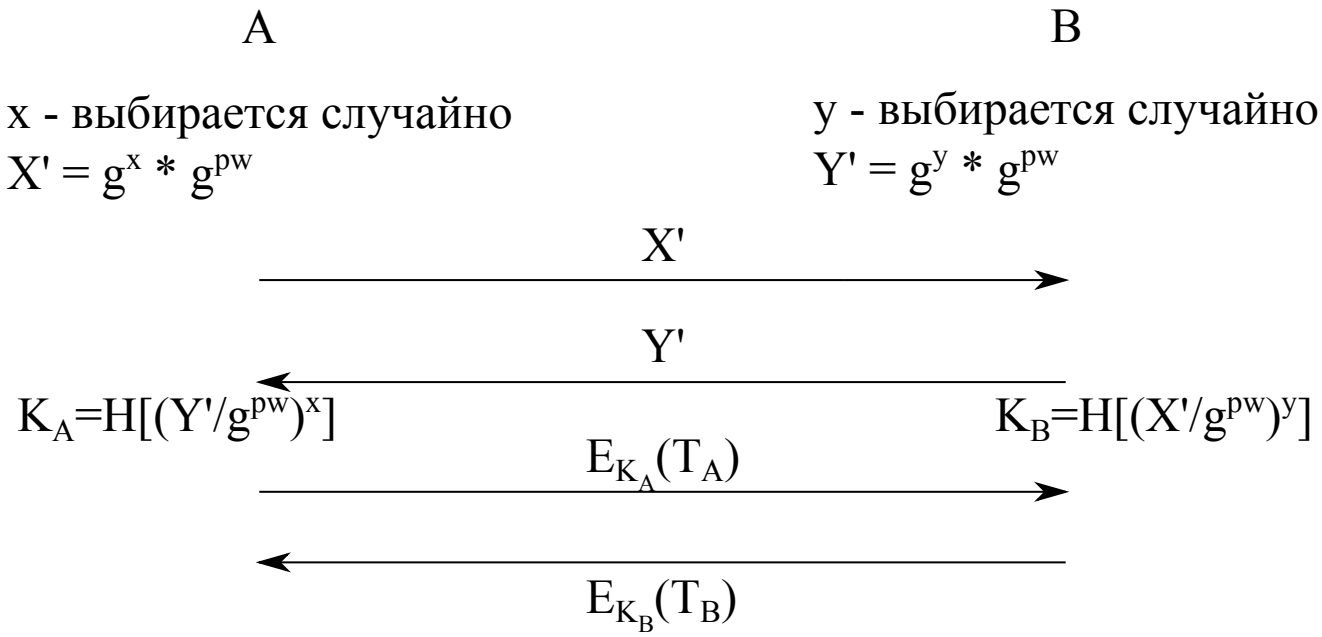
Пароль используется в качестве ”гаммы” при защите эфемерных ключей Диффи-Хеллмана. Сеансовый ключ не зависит от пароля. Здесь: $G = \langle g \rangle = \langle M \rangle = \langle N \rangle$.



КРИПТО ПРО

Пример 2: Какими должны быть используемые порождающие элементы?

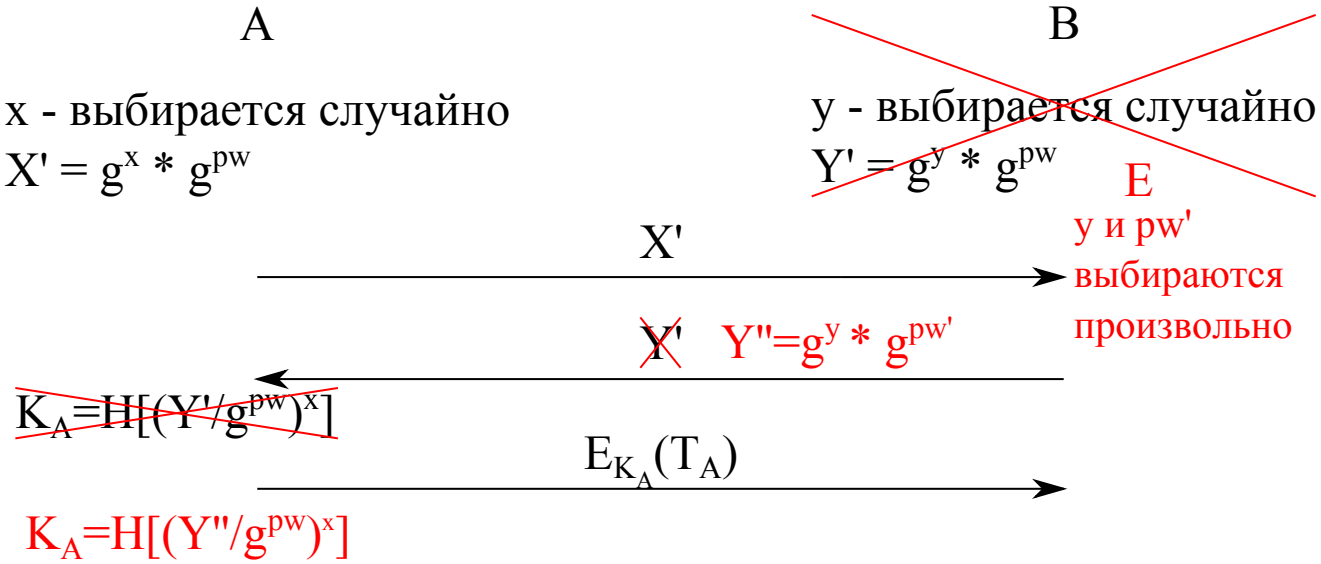
При формировании эфемерного открытого ключа и парольной ”маски” необходимо использовать разные порождающие элементы, причем дискретные логарифмы одного по основанию другого и наоборот должны быть неизвестны.



КРИПТО ПРО

Пример 2: Какими должны быть используемые порождающие элементы?

При формировании эфемерного открытого ключа и парольной ”маски” необходимо использовать разные порождающие элементы, причем дискретные логарифмы одного по основанию другого и наоборот должны быть неизвестны.



КРИПТО ПРО

Пример 2: Какими должны быть используемые порождающие элементы?

При формировании эфемерного открытого ключа и парольной ”маски” необходимо использовать разные порождающие элементы, причем дискретные логарифмы одного по основанию другого и наоборот должны быть неизвестны.

Первое описание протокола

1992 год: S.M. Bellovin, M. Merritt. «Encrypted Key Exchange: Password-based protocols secure against dictionary attacks».

Базовые модели противника

1993 год: M. Bellare, P. Rogaway. «Entity Authentication and Key Distribution». CTRYPTO'93.
1995 год: M. Bellare, P. Rogaway. «Provably Secure Session Key Distribution: the Three Party Case».

Используемая при обосновании модель противника

2000 год: M. Bellare, D. Pointcheval, P. Rogaway. «Authenticated key exchange secure against dictionary attacks».

Базовая работа в рамках модели

2005 год: M. Abdalla, D. Pointcheval. «Simple Password-Based Encrypted Key Exchange Protocols».

A	B	
$A_{ID} \longrightarrow$		
	$\longleftarrow (r, salt)$	
$Q' = r \cdot Q$		
$Q^A_{PW} = F(PW, salt, 2000) \cdot Q'$		
$\alpha \in_R [q-1]$		
$u_1 = \alpha \cdot P - Q^A_{PW} \longrightarrow$		
	Quit if $u_1 \notin E$	
	$Q_B = u_1 + Q_{PW}$	
	$\beta \in_R [q-1], R \in_R E^*, UKM \in_R [2^{128}-1]$	
	if $\frac{m}{q} Q_B = 0_E$, then $Q_B = R$	EKE_{KA}
	$K_B = H_{256}((UKM \cdot \frac{m}{q} \cdot \beta \mod q) Q_B)$	
	$\longleftarrow u_2 = \beta \cdot P + Q_{PW}, UKM$	
Quit if $UKM \notin [2^{128}-1]$ or $u_2 \notin E$		
$Q_A = u_2 - Q^A_{PW}, R \in_R E^*$		
if $\frac{m}{q} Q_A = 0_E$, then $Q_A = R$		
$K_A = H_{256}((UKM \cdot \frac{m}{q} \cdot \alpha \mod q) Q_A)$		
$C_A = E_{K_A}(T_A) \longrightarrow$ $I_A = Imit_{K_A}(T_A) \longrightarrow$		
	Verification: $D' = D_{K_B}(C_A) \stackrel{?}{=} T_A$	
	Verification: $Imit_{K_B}(D') \stackrel{?}{=} I_A$	
	$SID \in_R V^4_8$	EKE_{KC}
	$\longleftarrow C_B = E_{K_B}(T_B \| SID)$ $\longleftarrow I_B = Imit_{K_B}(T_B \| SID)$	
Verification: $D' = D_{K_A}(C_B) \stackrel{?}{=} T_B$		
Verification: $Imit_{K_A}(D') \stackrel{?}{=} I_B$		

КРИПТО ПРО

Общая схема обоснования

Протокол EKE разбит на два ”подпротокола”:

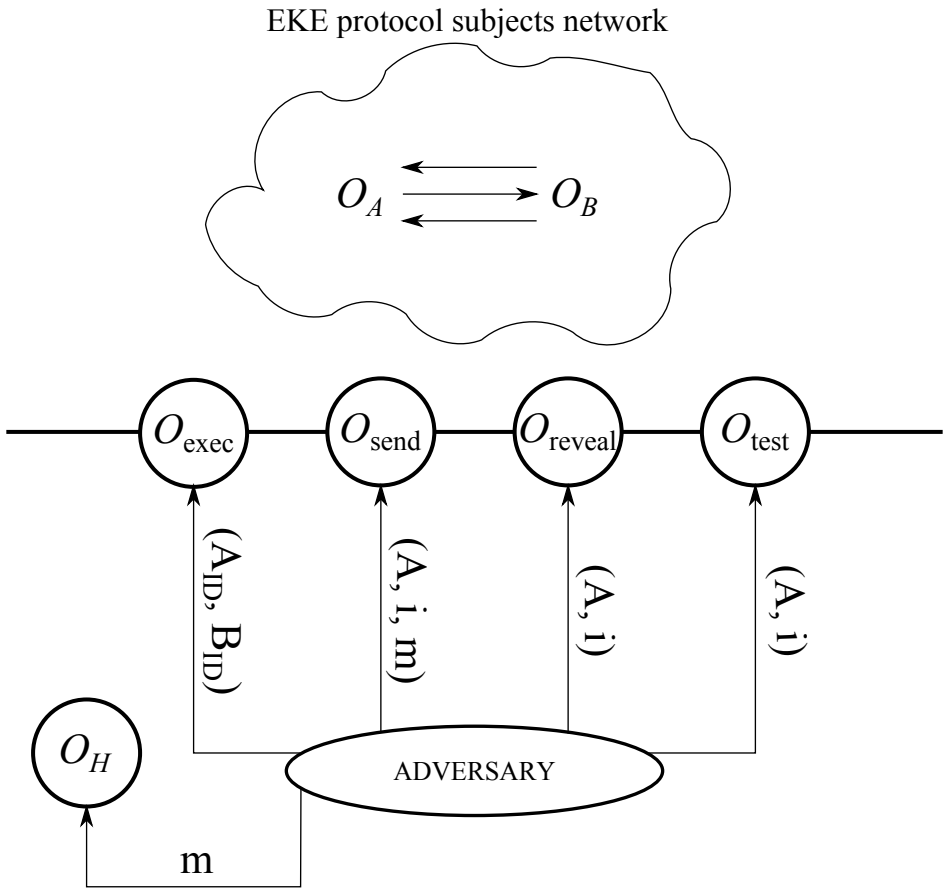
- EKE_{KA}
- EKE_{KC}

Стойкость протокола EKE_{KA} оценивается относительно угрозы отличения ключа выбранного сеанса от случайной строки

Стойкость протокола EKE оценивается относительно угрозы восстановления ключа выбранного сеанса. Доказательство существенно опирается на стойкость EKE_{KA} относительно угрозы отличения ключа от случайной строки.

КРИПТО ПРО

Модель противника



КРИПТО ПРО

Классическая схема получения нижних оценок

Предполагаем, что есть решатель задачи A, используем его в качестве черного ящика, для того чтобы решить задачу B. Получаем $T(B) \leqslant f(T(A))$, откуда заключаем, что $T(A) \geqslant f^{-1}(T(B))$.

Схема с постепенным изменением условий эксперимента

Предполагаем, что есть решатель S задачи A (например, задачи распознавания) и $P_{Exp(0)}(S)$ — преобладание решателя в условиях модельного эксперимента.

- Постепенно меняем условия эксперимента: $Exp(0) \rightsquigarrow Exp(1) \rightsquigarrow \ldots \rightsquigarrow Exp(N)$, где $P_{Exp(N)}(S) = 0$.
- Оцениваем $\delta_i = \left|P_{Exp(i)}(S) - P_{Exp(i-1)}(S)\right|$;
- Итоговая оценка: $P_{Exp(0)}(S) \leqslant \Sigma\delta_i$.

Для $q_{send} \geqslant 2$ и некоторого t, достаточного для осуществления одного взаимодействия с одним клиентом, справедливо неравенство:

$$\mathrm{Adv}_{\mathrm{EKE}_{KA}}(t, q_{send}) \geqslant \frac{1}{|\mathcal{D}|} - \frac{1}{q}.$$

Стойкость EKE_{KA} (отличение ключа от случайной строки)

Справедливо неравенство:

$$\mathrm{Adv}_{\mathrm{EKE}_{KA}}(t, q_H, q_{send}, q_{exec}, q_{reveal}) \leqslant$$
$$\leqslant \frac{2q_{send}}{|\mathcal{D}|} + \frac{(2q_{exec} + q_{send})^2}{q} + 2q_H \mathrm{Adv}_{CDH}(t + 2\tau q_{exec}) +$$
$$+ 2q_{send} \sqrt[4]{\sqrt{\mathrm{Adv}_{CDH}(8t + 8q_{S1}\tau + 2\Theta + O(q_H\tau))} + \frac{8q_H^4}{q}},$$

Стойкость $\mathrm{EKE}_{\mathrm{KA}}$ (угроза — вскрытие ключа)

Справедливо неравенство:

$$\mathrm{Adv}_{\mathrm{K,EKE}}(t, q_{\mathrm{exec}}, q_{\mathrm{send}}, q_{\mathrm{reveal}}, q_{\mathrm{H}}) \leqslant \leqslant 2\mathrm{Adv}_{\mathrm{K,EKE_{KA}}}(t, q_{\mathrm{exec}}, q_{\mathrm{send}}, q_{\mathrm{reveal}}, q_{\mathrm{H}}).$$

Стойкость EKE (угроза — вскрытие ключа)

Справедливо неравенство:

$$\mathrm{Adv}_{\mathrm{K,EKE_{KA}}}(t, q_{\mathrm{exec}}, q_{\mathrm{send}}, q_{\mathrm{reveal}}, q_{\mathrm{H}}) \leqslant \leqslant \frac{1}{2^n} + \mathrm{Adv}_{\mathrm{EKE_{KA}}}(t, q_{\mathrm{exec}}, q_{\mathrm{send}}, q_{\mathrm{reveal}}, q_{\mathrm{H}}).$$

КРИПТО ПРО

Спасибо за внимание! Вопросы?