Распределение ключей

2. Протоколы открытого распределения ключей

Атака «человек посередине»

Связываясь с Алисой, Мэллори по своим ролевым возможностям может выдавать себя за Боба, а связываясь с Бобом, она может выдавать себя за Алису, т.е. осуществлять так называемую атаку «человек посередине»:

1) Алиса отправляет Бобу свой открытый ключ. Мэллори перехватывает его и отсылает Бобу собственный открытый ключ от имени Алисы.
2) Боб отправляет Алисе свой открытый ключ. Мэллори перехватывает его и отсылает Алисе свой собственный открытый ключ от имени Боба.
3) Когда Алиса посылает сообщение Бобу, зашифрованное открытым ключом «Боба», Мэллори перехватывает его. Поскольку в действительности сообщение зашифровано её собственным открытым ключом, она расшифровывает его, снова шифрует открытым ключом Боба и переправляет Бобу.
4) Когда Боб отправляет Алисе сообщение, зашифрованное открытым ключом «Алисы», Мэллори перехватывает его. Поскольку в действительности сообщение зашифровано её собственным открытым ключом, она расшифровывает его, снова шифрует открытым ключом Алисы и переправляет Алисе.

Распределение ключей

2. Протоколы открытого распределения ключей

Протокол «станция-станция»

Обмен ключами Диффи-Хеллмана чувствителен к атаке «человек посередине», так же, как и протокол Хьюза. Одним из способов предотвратить такую атаку является подпись Алисой и Бобом сообщений, которые они посылают друг другу. Применяемый при этом протокол предполагает, что у Алисы есть открытый ключ Боба, а у Боба есть открытый ключ Алисы. Протокол имеет графическую схему обычного трёхпроходного протокола.

Вот как с помощью этого протокола можно провести алгоритм Диффи-Хеллмана, защищаясь от атаки «человек посередине».

Распределение ключей

2. Протоколы открытого распределения ключей

Протокол «станция-станция»

1. $A \to B$: $\{X = g^x \bmod p\}$, $1 < x < p$, x — секретное большое число Алисы.
2. 2.1. Боб выбирает случайное секретное большое число y $(1 < y < p)$;
   2.2. Боб вычисляет $Y = g^y \bmod p$ и $K = X^y \bmod p$;
   2.3. Боб подписывает X и Y, вычисляя подпись $S_B(X,Y)$;
   2.4. Боб шифрует подпись $E_K(S_B(X,Y))$ ключом K;
   2.5. $B \to A$: $\{Y, E_K(S_B(X,Y))\}$.
3. 3.1. Алиса вычисляет $K = Y^x \bmod p$;
   3.2. Алиса расшифровывает $D_K(E_K(S_B(X,Y))) = S_B(X,Y)$ подпись Боба и проверяет её, если подпись верна, то протокол продолжается;
   3.3. Алиса вычисляет свою подпись $S_A(X,Y)$ и шифрует её $E_K(S_A(X,Y))$;
   3.4. $A \to B$: $\{E_K(S_A(X,Y))\}$.

Боб расшифровывает и проверяет подпись Алисы, если она верна, то протокол заканчивается положительно.

Распределение ключей

3. Передача секретного ключа по открытому каналу

Открытый канал

Под открытым каналом подразумевается использование криптосистемы с открытым ключом. Одним из самых известным представителей этой системы является система RSA. Восстановим её алгоритмы.

Генерация ключей. Генерируются два больших безопасных простых числа p и q, которые держатся в секрете. Вычисляется натуральное число $n = pq$ и функция Эйлера $\varphi(n) = (p-1)(q-1)$. Выбирается случайное число e с условиями $1 < e < \varphi(n)$ и $(\varphi(n),\ e) = 1$. По расширенному алгоритму Евклида вычисляется $d = e^{-1} \bmod \varphi(n)$. Числа $\{n,\ e\}$ объявляются *открытым* (*публичным*) *ключом*, число d — *закрытым* (*секретным*) *ключом* пользователя системы. Все остальные параметры также держатся в секрете, либо уничтожаются.

Распределение ключей

3. Передача секретного ключа по открытому каналу

Открытый канал

Интерпретация файла открытого сообщения. Файл *открытого сообщения* M, прочитанный по битам и интерпретированный в этой записи как двоичная запись некоторого натурального числа, отождествляется с этим натуральным числом. Обратная операция преобразует любое натуральное число в некоторый файл. При этом формат файла становится безразличен. Поэтому в дальнейшем слова *сообщение* и *натуральное число* будут считаться тождественными. Система RSA требует выполнения условия $M < n$.

Распределение ключей

3. Передача секретного ключа по открытому каналу

Открытый канал

Алгоритмы шифрования и расшифрования.

$C = M^e \bmod n$ — криптограмма, $M = C^d \bmod n$ — открытое сообщение.

Протокол.

Простейший протокол передачи секретного ключа по открытому каналу является трёхпроходным и имеет графическую запись, показанную на рис. 2.

1. $A \rightarrow T$: Алиса запрашивает у Трента (ЦРК) открытый ключ Боба.
2. $T \rightarrow A$: Трент отвечает на запрос Алисы.
3. $A \rightarrow B$: Алиса генерирует случайный сеансовый ключ, шифрует его открытым ключом Боба и отправляет Бобу.
4. Боб расшифровывает копии сеансового ключа своим закрытым ключом.

Распределение ключей

3. Передача секретного ключа по открытому каналу

Открытый канал

На основе открытого канала построены, в частности, следующие протоколы аутентификации и обмена ключами:

- Протокол DASS;
- Протокол Деннинга-Сакко (Dorothy E. Denning, Giovanni Maria Sacco);
- Протокол Ву-Лама (T. Y. C. Woo, S. S. Lam);

Распределение ключей

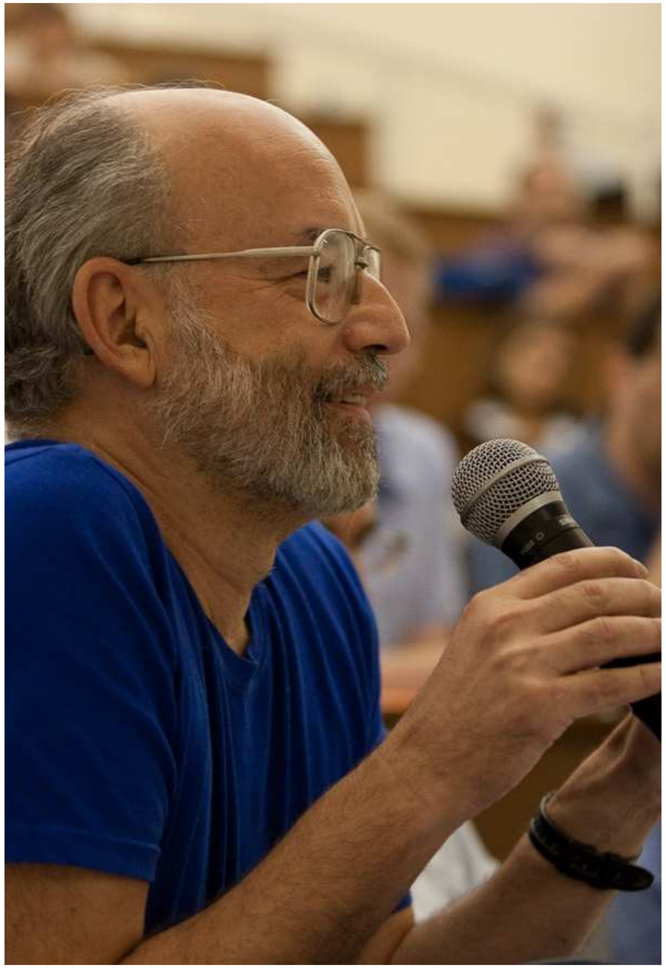
3. Передача секретного ключа по открытому каналу

Трехпроходный протокол Шамира

Этот изобретенный Ади Шамиром протокол, позволяет Алисе и Бобу безопасно обмениваться сеансовым ключом, не используя предварительного обмена ни секретными, ни открытыми ключами. Он предполагает использование коммутативного шифра относительно транспозиции ключей, т.е. для которого:

$$E_A(E_B(P)) = E_B(E_A(P)),$$

где использование ключей Алисы обозначается индексом A, а Боба — индексом B. Граф этого протокола изображён на рис. 4.



Распределение ключей

3. Передача секретного ключа по открытому каналу

Трехпроходный протокол Шамира

1. $A \to B$: $\{C_1 = E_A(K)\}$.
2. $B \to A$: $\{C_2 = E_B(C_1) = E_B(E_A(K))\}$.
3. $A \to B$: $\{C_3 = D_A(C_2) = D_A(E_B(E_A(K))) =$
   $= D_A(E_A(E_B(K))) = E_B(K)\}$.
4. B: $K = D_B(C_3) = D_B(E_B(K))\}$.

Ади Шамир (6 июля 1952 года, Тель-Авив, Израиль) — известный израильский криптоаналитик, учёный в области теории вычислительных систем, профессор информатики и прикладной математики в институте Вейцмана, лауреат премии Тьюринга. Член НАН Израиля (1998), иностранный член НАН США (2005)[2], Французской академии наук (2015)[3], Лондонского королевского общества (2018) и Американского философского общества (2019).

Распределение ключей

3. Передача секретного ключа по открытому каналу

Трехпроходный протокол Шамира

ЗАМЕЧАНИЕ. Не всякая коммутативная криптосистема сохраняет свою устойчивость в этом протоколе. Одноразовые блокноты обладают свойством коммутативности и обеспечивают абсолютную безопасность, но с описанным выше протоколом не работает. При использовании одноразового блокнота три шифртекста будут выглядеть следующим образом:

$$C_1 = K \oplus A;$$
$$C_2 = K \oplus A \oplus B;$$
$$C_3 = K \oplus B.$$

Ева, записав все эти три сообщения, которыми обмениваются Алиса и Боб, просто выполнит операцию *XOR* над всеми этими шифртекстами и восстановит сообщение:

$$C_1 \oplus C_2 \oplus C_3 = (K \oplus A) \oplus (K \oplus A \oplus B) \oplus (K \oplus B) = K.$$

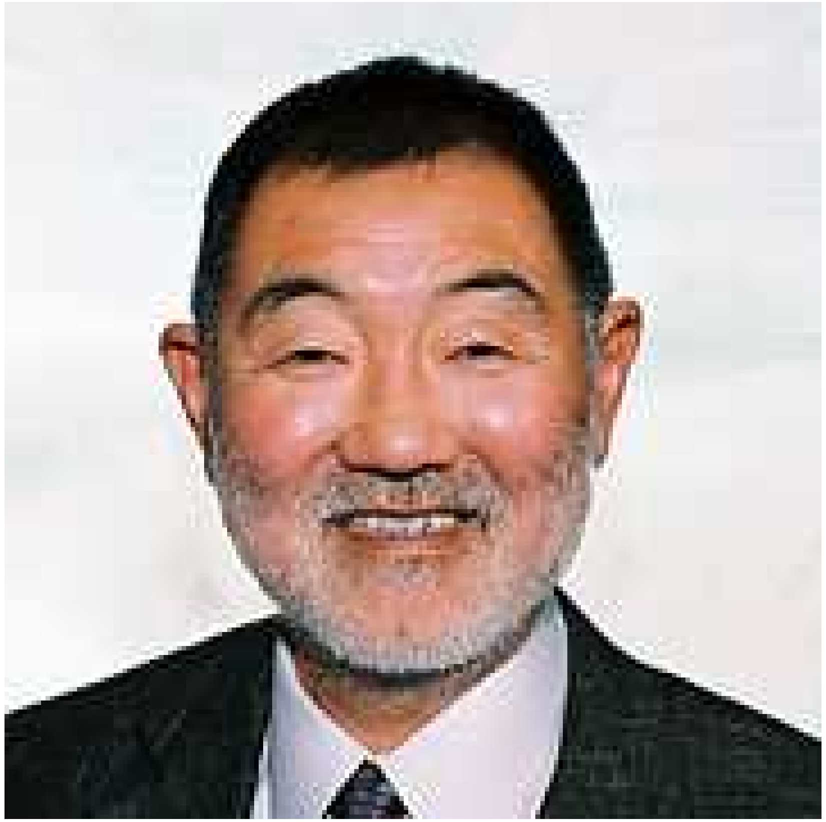
Распределение ключей

3. Передача секретного ключа по открытому каналу

Трехпроходный протокол Шамира

Криптосистема RSA вполне удовлетворяет требованиям этого протокола при условии, что Алиса и Боб используют один и тот же модуль *n*, а свои пары открытый/закрытый ключ держат в секрете.

Ади Шамир и, независимо, Джим Омура (Jim Omura), описали алгоритм шифрования, похожий на алгоритм RSA, который работает с описываемым протоколом.



Джимми К. Омура (родился 8 сентября 1940 года в Сан-Хосе, Калифорния) - инженер-электрик и теоретик информации . Он был профессором электротехники в Калифорнийском университете в Лос-Анджелесе в течение 15 лет. Он был избран членом Национальной инженерной академии в 1997 году и был введен в Зал инженерной славы Кремниевой долины в 2009 году.

Распределение ключей

3. Передача секретного ключа по открытому каналу

Трехпроходный протокол Шамира

Генерация ключей. Генерируется большое безопасное простое число p, которое может быть открытым для группы пользователей.

Функция Эйлера $\varphi(p) = p - 1$. Для генерации пары секретных ключей пользователя A выбирается случайное число e с условиями $1 < e < \varphi(p)$ и $(\varphi(p), e) = 1$. По расширенному алгоритму Евклида вычисляется $d = e^{-1} \bmod \varphi(p)$. Число e условно называются *открытым ключом* (или ключом шифрования), число d — *закрытым ключом* (или ключом расшифрования) пользователя A.

Распределение ключей

3. Передача секретного ключа по открытому каналу

Трехпроходный протокол Шамира

Алгоритмы (Шамира-Омура) шифрования и расшифрования.
$C = M^e \bmod p$ — криптограмма,
$M = C^d \bmod p$ — открытое сообщение, при условии $M < p$.

Данная криптосистема работает только при условии секретности обоих (открытый/закрытый) ключей, таким образом, она является ассиметричной, но не является криптосистемой с открытым ключом (с публичным ключом). В трёхпроходном протоколе Шамира эта криптосистема работает при дополнительном условии общего модуля p участвующих сторон. В этих условиях Ева не может получить M, не решив проблему дискретного логарифма.