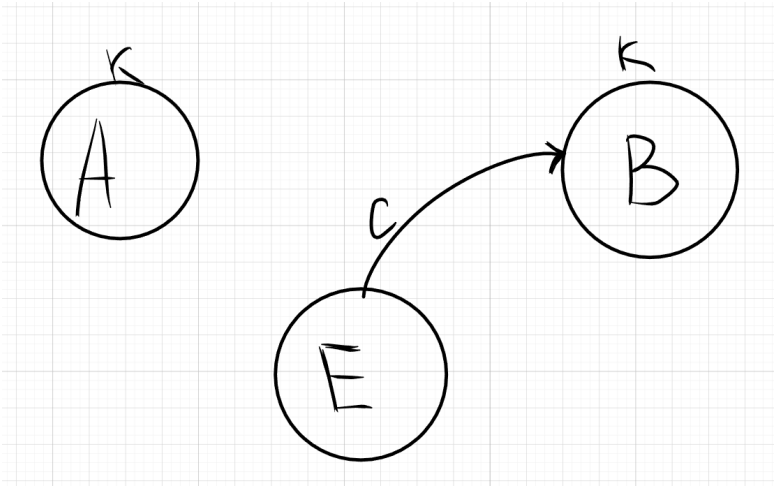
Модели атак: Имитация, Подмена и Навязывание

1 Модель атаки имитации



Известная криптосистема: $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E, D)$.

Два абонента (Алиса A и Боб B) обмениваются сообщениями с использованием секретного ключа k.

Криптоаналитик Ева перехватывает канал и отправляет Бобу криптограмму c. Атака имитации считается успешной, если:

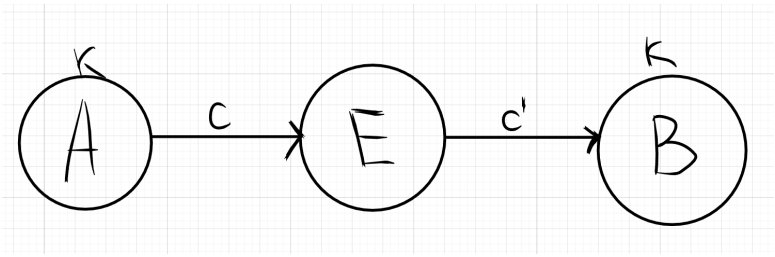
$$D(c, k) \in \mathcal{M}$$

Т.е. Боб принимает поддельное сообщение как настоящее.

Определение: Вероятность атаки имитации

$$P_{\text{им}} = \max_{c \in \mathcal{C}} P(D(c, k) \in \mathcal{M})$$

2 Модель атаки подмены



Известная криптосистема: $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E, D)$.

Ева перехватывает криптограмму c от Алисы и отправляет Бобу криптограмму $c' \neq c$.

Определение: Вероятность успеха атаки подмены

$$P_{\text{подм}} = \max_{\substack{(c,c')\in\mathcal{C}^2 \\ c\neq c'}} P(D(c',k)\in\mathcal{M} \mid D(c,k)\in\mathcal{M})$$

Определение: Вероятность навязывания

$$P_{\text{навяз}} = \max\{P_{\text{подм}}, P_{\text{им}}\}$$

Пусть все ключи равновероятны:

$$\forall k\in\mathcal{K} : P(K=k) = \frac{1}{|\mathcal{K}|}$$

3 Утверждение 1

$$P_{\text{им}} \geq \frac{|\mathcal{M}|}{|\mathcal{C}|}$$

Доказательство

Рассмотрим $c\in\mathcal{C}$. Определим:

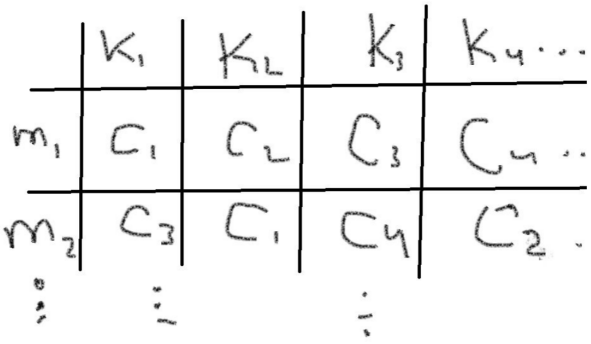
$$K(c) = \{k\in\mathcal{K} \mid D(c,k)\in\mathcal{M}\}$$

Так как ключи равновероятны:

$$P(D(c,k)\in\mathcal{M}) = \frac{|K(c)|}{|\mathcal{K}|}$$

$$P_{\text{им}} = \max_{c\in\mathcal{C}} \frac{|K(c)|}{|\mathcal{K}|} = \frac{1}{|\mathcal{K}|}\cdot\max_{c\in\mathcal{C}}|K(c)|$$

Рассмотрим таблицу шифрования:



Размер таблицы: $|\mathcal{M}|\cdot|\mathcal{K}|$
Также:

$$\sum_{c\in\mathcal{C}}|K(c)| = |\mathcal{M}|\cdot|\mathcal{K}|$$

Вопрос: почему сумма по всем $c\in\mathcal{C}$ значений $|K(c)|$ равна размеру таблицы?

$$\max_{c\in\mathcal{C}}|K(c)| \geq \frac{1}{|\mathcal{C}|}\sum_{c\in\mathcal{C}}|K(c)| = \frac{|\mathcal{M}|\cdot|\mathcal{K}|}{|\mathcal{C}|}$$

$$P_{\text{им}} \geq \frac{1}{|\mathcal{K}|}\cdot\frac{|\mathcal{M}|\cdot|\mathcal{K}|}{|\mathcal{C}|} = \frac{|\mathcal{M}|}{|\mathcal{C}|} \quad \blacksquare$$

4 Утверждение 2

$$P_{\text{подм}} \geq \frac{|\mathcal{M}| - 1}{|\mathcal{C}| - 1}$$

Доказательство

Для $c, c' \in \mathcal{C},\ c \neq c'$:

$$P(D(c', k) \in \mathcal{M} \mid D(c, k) \in \mathcal{M}) = \frac{|K(c) \cap K(c')|}{|K(c)|}$$

$$P_{\text{подм}} = \max_{(c,c') \in \mathcal{C}^2, c \neq c'} \frac{|K(c) \cap K(c')|}{|K(c)|}$$

Зафиксируем c:

$$\max_{c' \neq c} \frac{|K(c) \cap K(c')|}{|K(c)|} \geq \frac{1}{|K(c)|} \cdot \frac{\sum\limits_{c' \neq c} |K(c) \cap K(c')|}{|\mathcal{C}| - 1}$$

Подсчёт:

$$\sum_{c' \neq c} |K(c) \cap K(c')| = (|\mathcal{M}| - 1) \cdot |K(c)|$$

$$\Rightarrow P_{\text{подм}} \geq \frac{(|\mathcal{M}| - 1) \cdot |K(c)|}{|K(c)| \cdot (|\mathcal{C}| - 1)} = \frac{|\mathcal{M}| - 1}{|\mathcal{C}| - 1} \quad \blacksquare$$

5 Пример: Латинский квадрат

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

Латинский квадрат — таблица $n \times n$, в которой каждая строка и каждый столбец содержит все элементы множества $\{1, \ldots, n\}$ без повторений.

Пусть A — полунормализованный латинский квадрат (первая строка — тождественная перестановка).

Удалим первую строку: получим таблицу A' размером $(n-1) \times n$, где:

- $\mathcal{M} = \{m_1, \ldots, m_{n-1}\}$
- $\mathcal{K} = \{1, \ldots, n\}$
- $\mathcal{C} = \{1, \ldots, n\}$

Тогда:

$$P_{\text{им}} = \max_{c \in \mathcal{C}} \frac{|K(c)|}{|\mathcal{K}|} = \frac{n-1}{n} = \frac{|\mathcal{M}|}{|\mathcal{C}|}$$

$$P_{\text{подм}} = \max_{c \neq c'} \frac{|K(c) \cap K(c')|}{|K(c)|} = \frac{n-2}{n-1} = \frac{|\mathcal{M}| - 1}{|\mathcal{C}| - 1}$$

Таким образом, оценки из утверждений 1 и 2 являются точными и не могут быть улучшены.