Классификация

криптосистема

* по доступности информации
* по числу ключей
* по стойкости криптоалгоритма
* по используемым средствам шифрования
* по наличию сертификата

Атаки

* по доступу к открытому и зашифрованному тексту – только шифротекста;
* по контролю над процессом шифрования – активная, с имитацией и подменой сообщения;
* по объему необходимых ресурсов – память и время;
* по степени применимости к различным шифрам
* по используемым средствам
* по последствиям атаки;
* по возможности распараллеливания;

Взломщик

* по технической оснащенности
* по конечной цели
* по доступу к шифрующим средствам
* по уровню подготовки ;
* по первичной информации о средстве шифрования ;
* по возможности кооперации;

* , если атака c параметром  не применима к криптосистеме со значением параметра ;
* , если значение параметра криптосистемы снижает вероятность успешного применения атаки со значением параметра ;
* , если значение параметра криптосистемы не влияет на применимость атаки с параметром ;
* , если значение параметра криптосистемы указывает на то, что атака с параметром применима для взлома;

В случае с функцией взаимного влияния параметра злоумышленника b и параметра атаки a

* *,* если злоумышленник со значением параметра  гарантированно не будет использовать атаку со значением параметра ;
* *,* если значение параметра злоумышленника  снижает вероятность использования атаки со значением параметра ;
* *,* если значение параметра злоумышленника не влияет на вероятность использования атаки со значением параметра ;
* *,* если злоумышленник со значением параметра с большой вероятностью будет использовать атаку со значением параметра .

PRE

* - криптосистема ограниченного использования;
* - многоключевая;
* - доказуемо стойкая; (предположительно?)
* - программная;
* - сертифицированная;

Классическая криптосистема(предположим с использованием rsa алгоритма):

* – криптосистема общего пользования;
* - двухключевая;
* – доказуемо стойкая
* - программная; ?
* - сертифицированная;

Параметры атак (таблица 1)

|  |  |  |  |
| --- | --- | --- | --- |
|  | CCA - Chosen Cyphertext Attack | CPA - Chosen Plaintext Attack | SCA - Side channel attacks |
| A1 | Только шифротекста | Открытый текст | информация из побочных каналов |
| A2 | активная, с имитацией и подменой сообщения | пассивная | активная |
| A3 | память и время | данные | память, время и данные |
| A4 | универсальная | универсальная | универсальная |
| A5 | математические методы | математические методы | перехватчики физических параметров процесса шифрования |
| A6 | Нарушение  конфиденциальности | нарушение конфиденциальности | нарушение конфиденциальности |
| A7 | распределенная | не распределенная | распределенная |

Взаимное влияние параметров PRE на параметры атак значения через ; в порядке CCA, CPA, SCA

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **PRE** | A1 | A2 | A3 | A4 | A5 | A6 | A7 |
| C1 | 0.1;0.3;0.5 |  |  |  |  |  |  |
| C2 |  |  |  |  |  |  |  |
| C3 |  |  |  |  |  |  |  |
| C4 |  |  |  |  |  |  |  |
| C5 |  |  |  |  |  |  |  |
| **RSA** |  | | | | | | |
| C1 |  |  |  |  |  |  |  |
| C2 |  |  |  |  |  |  |  |
| C3 |  |  |  |  |  |  |  |
| C4 |  |  |  |  |  |  |  |
| C5 |  |  |  |  |  |  |  |

Классификация взломщиков

|  |  |  |
| --- | --- | --- |
|  | Взломщик 1 | Взломщик 2 |
| B1 | сеть ЭВМ | персональный компьютер |
| B2 | полный взлом алгоритма | обнаружение слабости в алгоритме |
| B3 | “внешний” нарушитель | “внутренний” нарушитель |
| B4 | программирование | математический аппарат |
| B5 | криптограф | пользователь |
| B6 | коллектив | одиночка |

взаимное влияние параметра злоумышленника b и параметра атаки CCA(в формате взломщик 1; взломщик 2)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CCA** | A1 | A2 | A3 | A4 | A5 | A6 | A7 |
| B1 |  |  |  |  |  |  |  |
| B2 |  |  |  |  |  |  |  |
| B3 |  |  |  |  |  |  |  |
| B4 |  |  |  |  |  |  |  |
| B5 |  |  |  |  |  |  |  |
| B6 |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CPA** | A1 | A2 | A3 | A4 | A5 | A6 | A7 |
| B1 |  |  |  |  |  |  |  |
| B2 |  |  |  |  |  |  |  |
| B3 |  |  |  |  |  |  |  |
| B4 |  |  |  |  |  |  |  |
| B5 |  |  |  |  |  |  |  |
| B6 |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SCA** | A1 | A2 | A3 | A4 | A5 | A6 | A7 |
| B1 |  |  |  |  |  |  |  |
| B2 |  |  |  |  |  |  |  |
| B3 |  |  |  |  |  |  |  |
| B4 |  |  |  |  |  |  |  |
| B5 |  |  |  |  |  |  |  |
| B6 |  |  |  |  |  |  |  |