

**MOSCOW OF UNIVERSITY OF THE MINISTRY OF INTERNAL AFFAIRS**

**OF THE RUSSIAN FEDERATION NAMED AFTER V. Y. KIKOT**

Department of foreign languages

Discipline: English

Report: “ Cryptography“

Performed: Checked

by students of by senior lecturer of

2st year Department of

platoon #228 Major

A. E. Pokinen V.N. Kulikov

Moscow 2018

**Introduction to Cryptography**

Definitions

* + Cryptography = the science (art) of encryption
  + Cryptanalysis = the science (art) of breaking encryption
  + Cryptology = cryptography + cryptanalysis

Cryptography Goals

1. Encryption – Prevent Eve from intercepting message
2. Authentication – Prevent Eve from impersonating Alice

Symmetric (secret) Key

* + Alice and Bob share a secret key, Kab
  + Encryption – Plaintext message is encrypted and decrypted with Kab
  + Authentication – Alice proves to Bob that she knows Kab (e.g. a password)

Cryptographic Attacks

* + Ciphertext only: attacker has only ciphertext.
  + Known plaintext: attacker has plaintext and corresponding ciphertext.
  + Chosen plaintext: attacker can encrypt messages of his choosing.
  + Distinguishing attack: an attacker can distinguish your cipher from an ideal cipher (random permutation).
  + A cipher must be secure against all of these attacks.

Provable Security

* + 1. There is no such thing as a provably secure system.
    2. Proof of unbreakable encryption does not prove the system is secure.
    3. The only provably secure encryption is the one time pad: C = P + K, where K is as long as P and never reused.
    4. Systems are believed secure only when many people try and fail to break them.

Cryptographic Algorithms

1. Block ciphers (secret/symmetric key)
2. Hashes
3. MAC (keyed hashes)
4. Diffie-Hellman key exchange
5. RSA (public key encryption and digital signature)
6. ElGamal digital signature

Hash Applications

* 1. Faster digital signatures: Alice signs h(P) instead of P.
  2. Password verification (e.g. UNIX) without storing passwords.
  3. Strong pseudo-random number generation.
  4. Message Authentication Code (MAC).
  5. Summary
  6. Cryptography is hard
  7. Security can not be proven.
  8. Even expertly designed systems have weaknesses.
  9. Designing your own encryption algorithm would be foolish.
  10. Cryptography is not the answer
  11. Most attacks do not involve breaking encryption.
  12. Prevent, Detect, Recover
  13. Cryptography is only for prevention

**Введение в криптографию**

Определения:

1. Криптография = наука (искусство) шифрования
2. Криптоанализ = наука (искусство) взлома шифрования
3. Криптология = криптография + криптоанализ

Цели криптографии:

* Шифрование - Предотвратить перехват сообщения Евой
* Аутентификация - не дать Еве выдать себя за Алису

Симметричный (секретный) ключ

* Алиса и Боб делятся секретным ключом, Каб
* Шифрование - текстовое сообщение шифруется и дешифруется с помощью Kab
* Аутентификация - Алиса доказывает Бобу, что она знает Каб (например, пароль)

Криптографические атаки

1. Только зашифрованный текст: у злоумышленника есть только зашифрованный текст.
2. Известный открытый текст: у злоумышленника есть открытый текст и соответствующий зашифрованный текст.
3. Выбранный открытый текст: злоумышленник может зашифровать сообщения по своему выбору.
4. Отличительная атака: атакующий может отличить ваш шифр от идеального (случайная перестановка).
5. Шифр должен быть защищен от всех этих атак.

Обеспечиваемая безопасность

Обеспечение безопасности:

* Нет такой вещи, как доказуемо безопасная система.
* Доказательство нерушимого шифрования не доказывает безопасность системы.
* Единственное доказуемо безопасное шифрование - это временная клавиатура: C = P + K, где K равно P и никогда не используется повторно.
* Системы считаются безопасными только тогда, когда многие пытаются и не могут их сломать.

Криптографические алгоритмы

* Блочные шифры (секретный / симметричный ключ)
* Хэш
* MAC (хеши с ключами)
* Обмен ключами Диффи-Хеллмана
* RSA (шифрование с открытым ключом и цифровая подпись)
* ElGamal цифровая подпись

Хэш-приложения

* Более быстрые цифровые подписи: Алиса подписывает h (P) вместо P.
* Проверка пароля (например, UNIX) без хранения паролей.
* Сильная генерация псевдослучайных чисел.
* Код аутентификации сообщения (MAC).

Подводя итоги

* Криптография это сложно
* Безопасность не может быть доказана.
* Даже опытно спроектированные системы имеют недостатки.
* Создание собственного алгоритма шифрования было бы глупо.
* Криптография не ответ
* Большинство атак не включают взлом шифрования.

Предотвратить, обнаружить, восстановить