دانشگاه بین المللی امام خمینی قزوین

دانشکدهٔ فنی و مهندسی

مبانی امنیت اطلاعات

(سومین ترم کرونا)

رمزنگاری

نستوه طاهری جوان

nastooh@aut.ac.ir

مقدمه

- ✓ بحث آزاد در مورد مفهوم محرمانگی
- ✓ بحث آزاد در مورد تاریخچهٔ رمزنگاری در سیستم های نظامی

تعریف های بنیادین

- Plain Text
  - دادهٔ اصلی
- Cipher Text
  - حاصل رمزنگاری
- Encryption
  - عملیات رمزگذاری
- Decryption
  - عملیات رمزگشایی
- Key
  - دادهٔ کمکی

nastooh@aut.ac.ir

طبقه بندی الگوریتم های رمزنگاری

- ✓ رده های اصلی رمزنگاری
  - ○ الگوریتم های محدود

    اصل: محرمانه نگه داشتن خود الگوریتم
  - ○ الگوریتم های مبتنی بر کلید
    - متقارن
      - جانشینی
      - جایگشتی
    - نامتقارن

روش های جانشینی

- ✓ هر حرف (یا گروهی از حروف) با یک حرف (یا گروهی از حروف) دیگر جایگزین می گردد.
  - مانند روش سزار (یا Shift by K)
    - روال کار

      جایگزینی هر حرف، با K حرف جلوتر

    - مثال:
      - Plain TXT: HELLO
      - key: 3
      - Cipher TXT: KHOOR
    - تعداد حالت های کلید
    - در هم شکستن

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

nastooh@aut.ac.ir

روش های جانشینی

- ✓ بهبود روش سزار
  - ○ جایگزینی هر حرف با یک حرف دلخواه!
    - تعریف کلید
    - مثال:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

- تعداد حالت های کلید
- در هم شکستن

nastooh@aut.ac.ir

روش های جانشینی

- ✓ تاملی در مورد تحلیل آماری رمزها

بحث آزاد و مهم

nastooh@aut.ac.ir

روش های جایگشتی

- ✓ جابجایی ترتیب سمبل ها (و ثابت ماندن شکل سمبل ها، برعکس جانشینی)
  - مثال یک: نوشتن یک متن در یک ماتریس به صورت سطری، و بازنویسی آن از ستون ها
    - کلید چیست؟
  - مثال دو: ابزار زیر را تحلیل کنید.

nastooh@aut.ac.ir

روش One Time Pads

- ✓ روش کار
  - XOR کردن متن اصلی با کلید، بیت به بیت
  - مثال:

P.T.: 1 1 0 0 1 0 1 0 1 0
K: 0 1 1 0 1 1 0 1 1 1
C.T: 1 0 1 0 0 1 1 1 0 1
K: 0 1 1 0 1 1 0 1 1 1
P.T.: 1 1 0 0 1 0 1 0 1 0

- استفاده از کلید
- در هم شکستن

- و اما: تبادل کلید؟

nastooh@aut.ac.ir

منابع

[1] William Stallings, “Computer Security,” 3th ed. (Download Link)

[2] William Stallings, “Cryptography and Network Security,” 7th ed. (Download Link)

[3] William Stallings, “Network Security Essentials,” 4nd ed. (Download Link)

پایان

nastooh@aut.ac.ir