

رمز گاری - رمز گشایی

معمولا یکی از فصلهای کتاب رمز گذاری بدون ذکر ساختمان داده ها درباره

رمز گذاری و رمز گشایی است .
پارسی کتاب

رمز گذاری و رمز گشایی را میتوان کنار اعمال دیگری که روی

رشته ها انجام میشود قرار داد از قبیل: الحاق و محاسبه

طول و ... در رمز گذاری هدف تغییر دادن متن ساده به

متنی غیر قابل درک و سری است که در صورت لزوم میتوان

آن را به متن اولیه تبدیل کرد (رمز گشایی).

ساده ترین عملی که برای رمز گذاری انجام میشود جانشینی

است. در این روش هر کاراکتر با کاراکتر دیگری تعویض

میشود. به عنوان مثال کد اسکی هر کاراکتر از ۲۵۵ کم

میشود. به این ترتیب کاراکتر A(65) به ۲۵۵-۶۵=۱۹۰ تبدیل

میشود. عمل جانشینی را میتوان با استفاده از یک جدول نیز

انجام داد. این جدول یک تناظر یک به یک بین کاراکتر ساده

و کاراکتر رمزی آن برقرار میکند. برای مثال جدول زیر را

در نظر بگیرید

A B C D E F

H T J K A Y

در این صورت اگر متن ساده برابر با CAD باشد به متن

رمزی JHK تبدیل میشود.

بنظر نمیرسد چنین استفاده های ساده ای از روش جانشینی

چندان قابلیت اطمینانی داشته باشد. برای مثال در مورد

فرمولی که ما استفاده کردیم، اگر کسی که قصد

رمزگشایی داشته باشد فقط یک کاراکتر از متن را بداند

میتواند الگوریتم رمزگذاری ما را کشف کند.

روش دیگر رمزگذاری روش جایگشت است. در این روش

کاراکترهای متن اصلی جابجا میشوند. برای مثال کاراکتر اول

به مکان سوم و کاراکتر سوم به مکان دوم و دومی به جای

کاراکتر اول منتقل میشوند. یعنی رشته ali به lia تبدیل

میشود.

با ترکیب کردن این دو روش میتوان الگوریتم های پیچیده ای

ایجاد کرد. اما همه آنها به شدت آسیب پذیر خواهند بود.

تصور کنید که علی میخواهد یک نامه به مریم بفرستد (وای

وای وای!) که متن آن بسیار محرمانه است! او برنامه

رمزگشا را به مریم میدهد و نامه را برای او میفرستد. تا

اینجای کار ایرادی ندارد ولی از آنجا که علی برای نرگس هم

نامه‌های محرمانه ای میفرستد باید برنامه رمزگشا را به

نرگس هم بدهد. حالا اگر نرگس نامه‌ای که علی به مریم

فرستاده بود بدست بیاورد میتواند به راحتی آن را کشف

رمز کند. و مگر خدا به داد علی برسد!

اجازه بدهید فرمول جانشینی را کمی تغییر دهیم ($chr + X$)

$(mod\ 255)$ در اینجا chr کاراکتری است که باید رمز شود و

X عددی است که کاربر وارد میکند. به این ترتیب کاربری

که میخواهد متن را کشف رمز کند باید مقدار X ای که متن

با استفاده از آن رمز شده است را بداند. در این قبیل

الگوریتم‌ها به X "کلید خصوصی" میگویند. و به خود الگوریتم

"الگوریتم رمزگذاری کلید خصوصی یا الگوریتم رمزگذاری

مقارن" میگویند. مقارن به این دلیل که کلید رمزگذاری و

رمزگشایی یکی است.

از جمله الگوریتم‌های رمزگذاری کلید خصوصی میتوان به

"استاندارد رمزگذاری داده‌ها (Data Encryption

Standard) اشاره کرد.

DES :

این الگوریتم یکی از پر استفاده‌ترین الگوریتم‌های رمزگذاری

است. اگر نگاهی به الگوریتم جانشینی اصلاح شده ای که

سپس متن ۶۴ بیتی به دو بخش ۳۲ بیتی تبدیل میشود که

آنها را L_0 و R_0 مینامیم. پس از آن با استفاده از کلید K_1 و

تابع R_0 ، F رمز میشود $F(R_0, K_1)$ و در مرحله بعد از آن (

$F(R_0, K_1)$ با L_0 یای انحصاری (XOR) میشود و R_1 را برای

مرحله دوم ایجاد میکند. اما مرحله دوم نیاز به L_1 نیز دارد.

L_1 برابر با R_0 است. این عمل تا مرحله ۱۶ ادامه میابد. پس

از مرحله آخر دو بلوک ۳۲ بیتی به هم متصل میشوند و یک

بلوک ۶۴ بیتی رمز را ایجاد میکنند.

این الگوریتم سال ۱۹۷۷ در شرکت IBM ایجاد شد و سازمان

دفاع آمریکا آن را در اختیار گرفت. شماره استاندارد آن

ANSI X3.92 و X3.106 است.

در سال ۱۹۹۷ مالک RSA (یک الگوریتم رمزگذاری کلید

عمومی) جایزه ۱۰۰۰۰ دلاری برای شکستن DES تایین کرد.

یک شرکت با استفاده از ۱۴۰۰۰ کامپیوتر در اینترنت اقدام به

آزمایش کلید برای یک متن رمز شده DES کرد و پس از

آزمایش تنها ۱۸ گرادیلیون (۱۸ با ۲۴ تا صفر) از ۷۲ گرادیلیون

موفق شد رمز را کشف کند. امروزه احتمالاً تعداد کمی از

پیغامهایی که با استفاده از DES فرستاده میشوند با این

روش شکسته میشوند.

درمورد استاندارد شدن این الگوریتم هم بحث های زیادی

شده است که آیا کلید ۴۸ بیتی که در جایگشت اولیه

استفاده میشود به اندازه کافی طولانی هست؟ و اینکه آیا

کلیدهای جانشینی به اندازه کافی پیچیده هستند؟

DES در VS.Net

VS.Net از تعدادی از الگوریتمهای رمزگذاری مهم از جمله

DES پشتیبانی میکند.

مثالی که در زیر آمده است یک متن را رمز کرده و در

TextBox2 مینویسد. پس از آن آن متن را رمزگشایی کرده

و در TextBox1 مینویسد. کلید خصوصی و بردار اولیه

تصادفی انتخاب میشوند.

parsi e-book
WWW.PARSIBOOK.4T.COM

```

Dim des As New
DESCryptoServiceProvider()

Dim inputArray() As Byte =
System.Text.Encoding.UTF8.GetBytes("D
ata Encryption")
Dim ms As New IO.MemoryStream()

Dim encCS As New CryptoStream(ms,
des.CreateEncryptor(),
CryptoStreamMode.Write)

Dim key() As Byte = des.Key
Dim IV() As Byte = des.IV
encCS.Write(inputArray, 0,
inputArray.Length)

encCS.FlushFinalBlock()

TextBox2.Text =
System.Text.Encoding.UTF8.GetString(m
s.ToArray)

```

```
ms.Seek(0, IO.SeekOrigin.Begin)

Dim decCS As New CryptoStream(ms,
des.CreateDecryptor(key, IV),
CryptoStreamMode.Read)
Dim sr As New IO.StreamReader(decCS)
TextBox1.Text = sr.ReadToEnd()
```



parsi e-book
WWW.PARSIBOOK.4T.COM