دانشگاه زنجان

دانشکده مهندسی

گروه برق

پایان نامه کارشناسی

گرایش: الکترونیک

عنوان:

امنیت در شبکه های کامپیوتری

استاد راهنما:

جناب آقای دکتر محمدی

نگارش:

حمید صالحی راد

تاریخ دفاعیه : **بهمن ۱۳۸۹**

فهرست :

فصل اول

۱-۱ - تاریخچه رمزنگاری :

کلمه رمزنگاری[۱] از لغتی یونانی به معنای محرمانه نوشتن متون برداشت شده و پیشینه ای طولانی دارد . از نظر تاریخی نظامیان ، هیات های سیاسی ، خاطره نویسان و عشاق از رمزنگاری بیشتر استفاده کرده و در گسترش آن نقش بیشتری داشته اند ولی نقش نظامیان پر رنگ تر بوده است . تا قبل از ابداع کامپیوتر پیامدها توسط یک کارمند رمز و ارسال می شدند . و این روش مشکلاتی داشت . از قبیل :

۱. تاثیر مستقیم سرعت کارمند در حجم اطلاعات ارسالی
۲. محدودیت در تغییر روش رمزنگاری به دلیل نیاز مجدد به آموزش افراد
۳. فاش شدن روش رمزنگاری در صورت دستگیری افراد مطلع از آن

یکی از علل شکست ژاپن در جنگ جهانی دوم استفاده ارتش آمریکا از یک رمزنگاری که بر پایه ی یک لهجه محلی سرخپوستان به نام Navajo بود . این زبان یک لهجه ی بسیار شدید داشت و هیچ یک از ژاپنی ها هرگز نتوانستند قادر به درک این رمز بشوند.

---

۱. Cryptography

۱-۲ - مقدمه ای بر رمزنگاری :

اگر بخواهیم رمزنگاری را به صورت ریاضی بیان کنیم ، می توان پارامترهای زیر را در نظر گرفت :

۱. متن آشکار[۱] : پیامی است که می خواهیم آن را رمزنگاری کنیم (P)

۲. کلید[۲] : پارامتر تابع رمزنگاری (K)

۳. متن رمز[۳] : نتیجه عملیات رمزنگاری (C)

با استفاده از پارامترهای بالا می توان تابع ریاضی زیر را برای رمزنگاری در نظر گرفت :

$$C = \mathrm{E_k(P)}$$

معنای این تابع این است که رمزنگاری بر روی متن آشکار P و توسط تابع E با پارامتر K انجام شده است و متن رمز C بدست آمده است .

اگر بتوان معکوس تابع رمزنگاری را بدست آورد ، قادر به یافتن متن آشکار خواهیم شد.

$$P = \mathrm{D_k(E_k(P))}$$

از آنجایی که محرمانه نگه داشتن روش رمزنگاری خیلی مشکل است ، به عنوان یکی از قواعد اساسی در رمزنگاری ، شخص رمزنگار باید این فرض را بپذیرد که همه افراد روش رمزنگاری یعنی تابع E و روش رمزگشایی یعنی تابع D را می دانند و تنها کلید رمز k پنهان است .

---

۱. Plaintext
۲. Key
۳. Ciphertext

کلید رمز یک رشته کاراکتر است که در تابع رمزنگاری مورد استفاده قرار می گیرد وی می تواند تغییر کند . این بیان ساده ، یکی از اصول اساسی رمزنگاری به نام اصل کرکهف است .

اصل کرکهف : همه الگوریتم های رمزنگاری باید آشکار و عمومی باشند و فقط کلید رمز محرمانه است . فایده آشکارسازی الگوریتم رمزنگاری به چالش کشیدن متخصصان رمزنگاری برای شکستن این الگوریتم و پی بردن به نقاط ضعف و قوت این الگوریتم می باشد . [۱]

با توجه به آشکار بودن الگوریتم رمزنگاری ، تضمین غیر قابل شکسته بودن یک پیام رمز شده منوط به انتخاب یک کلید رمز مناسب و با طول زیاد است . در زیر به بیان روش های رمزنگاری اطلاعات می پردازیم :

۱-۳ - رمزنگاری جانشینی :

در این روش یک حرف با حرفی دیگر یا گروهی از حروف با گروهی دیگر جایگزین می شود . گفته می شود سزار اولین بار با شیفت دادن هر حرف الفبا به میزان سه حرف ، از این روش بهره گرفت . وی حرف a را به D ، حرف b را با e و . . . جابجا کرد و به عنوان مثال در روش او ، کلمه attack به DWWDFN تبدیل گشت . این روش را که در آن یک حرف با یک حرف دیگر جایگزین می شود ، سیستم جانشینی تک حرفی گویند .

هرچند برای رمز شکنی متون رمز شده به این روش باید ! ۲۶ حالت مختلف در نظر گرفته شود ، اما متخصصان رمز شکنی ، برای گشودن این رموز از ویژگی های آماری زبان های طبیعی استفاده می کنند .

مـــثلا در زبـــان انگلیســـی حـــروف e ، t ، o ، a ، n دو حرفـــی هـــای th ، in ، er ، re و سه حرفی های the ، ing ، and بیشترین تکرار را دارند .

رمـز شـکنی کـه مـی خواهـد یـک متنـی را کـه از طریـق رمزنگـاری جانشـینی رمـز شـده اسـت ، رمزگشـایی کنـد بـه جـای در نظـر گـرفتن !۲۶ حالـت مختلـف کـه آزمـون آنهـا چنـد سـال طـول مـی کشـد ، سـعی مـی کنـد بیشـترین حروفـی را کـه در مـتن ذکـر شـده بیابـد . اولـین حـرف را بـا حـرف e جـایگزین مـی کنـد ، دومـی را بـا t و . . . سـپس بـه دنبـال سـه حرفـی the مـی گـردد . دو حـرف t و e را قـبلا یافتـه و حـرف جدیـدی کـه در e . . . t قـرار دارد احتمـالا h اسـت . سـپس بـه دنبـال حـرف a در میـان چهـار حرفـی هـای t . . . th مـی گـردد و بـدین طریـق مـی توانـد حـروف اصلی را از جایگزینان آن تشخیص دهد .

روش هوشـمندانه ی دیگـری کـه وی مـی توانـد اتخـاذ کنـد ، حـدس زدن یـک کلمـه در یـک مـتن اسـت . بـه عنـوان مثـال فـرض کنیـد کـه یـک مـتن رمـز شـده کـه مربـوط بـه ایـران اسـت بـه شخصـی داده شـده اسـت . وی حـدس مـی زنـد کـه کلمـه IRANIAN در آن متن وجود دارد .

OLXY	YXYA	GSTJ	CQVU	ZMWO	ZWAK
VGUS	VUSZ	QJMK	QMKA	AYYY	MNIS
JDST	JQUU	STJC	XQBN	BYYC	

بـا توجـه بـه کلمـه ی مـورد شـک او (IRANIAN) وی ابتـدا بـه دنبـال دو حرفـی در مـتن مـی گـردد کـه بـه فاصـله سـه حـرف از یکـدیگر تکـرار شـده انـد . مـوارد ۱۷ و ۲۱ ، ۲۵ و ۲۹ ، ۴۹ و ۵۳ و ۳۳ و ۳۷ دارای ایـن ویژگـی هسـتند . بعـد او توجـه مـی کنـد کـه در کلمـه IRANIAN دو حرفـی ۳ و ۴ و ۵ و ۶ بـه فاصـله یـک حـرف از

یکدیگر تکرار شده اند . در این متن رمز شده ، موارد ۳ ، ۴ و ۶ ، ۷ و ۳۵ و ۳۶ و ۳۸ ، ۳۹ و ۲۷ ، ۲۸ و ۳۰ ، ۳۱ در این رابطه صدق می کنند .

با توجه به دو مورد بالا ، می توان یافت که کلمه IRANIAN در جایگاه ۳۹ ـ۳۳ و به صورت QQJMKQMK در متن رمز شده است . [۱, ۲]

۱-۴ - رمزنگاری جایگشتی :

در این روش ، جای حروف عوض می شود ولی شکل آنها تغییر نمی کند . برای رمز کردن یک متن به صورت جایگشتی مراحل زیر را باید انجام داد .

۱) انتخاب کلید رمز

۲) شماره گذاری ستون ها براساس تقدم الفبایی حروف کلید رمز

۳) نوشتن متن اصلی به صورت افقی در زیر کلید رمز

۴) کامل کردن ماتریس با اضافه کردن حروف دلخواه در صورت نیاز

روش بالا یک روش کلی و عمومی برای رمزنگاری به صورت جایگشتی است و برای توضیح بیشتر ، مثال زیر را در نظر می گیریم .

فرض کنید متن زیر قرار است توسط رمزنگاری جایگشتی و با کلید رمز your name ارسال شود .

When Sun Sets Start attack with all power

با توجه به مراحل بالا ، ابتدا باید کلید رمز را شماره گذاری کرد .

y o u r n a m e

۸ ۵ ۷ ۶ ۴ ۱ ۳ ۲

حال با استفاده از کلید رمز فوق ، یک ماتریس شامل ۸ ستون تشکیل می دهید . و بعد متن آشکار را در زیر آن به صورت افقی می نویسیم .

y	o	u	r	n	a	m	e
۸	۵	۷	۶	۴	۱	۳	۲
w	h	e	n	s	u	n	s
e	t	s	s	t	a	r	t
a	t	t	a	c	k	w	i
t	h	a	l	l	p	o	w
e	r	a	b	c	d	e	f

حال براساس ترتیب هر ستون ، متن رمز شده را می نویسیم .

uakpdstiwfnrwoestcLchtthrnsaLbestaaweate

رمزنگاری متن بالا تمام شده است . می بینیم که شکل حرف جا به جا نشده است و فقط جای آنها در متن عوض شده .

حال که متن رمزنگاری شد می خواهیم بدانیم که یک رمز شکن برای رسیدن به متن آشکار با استفاده از این متن رمز شده چه باید کند .

۱) حصول اطمینان از اینکه این متن توسط رمزنگاری جایگشتی رمز شده است.

۲) تشخیص تعداد ستون ها

۳) بدست آوردن ترتیب ستون ها

۱. اگر متن رمز شده را بررسی کنید خواهید یافت که حروف t ، a ، e ، i و . . . در متن زیاد تکرار شده اند و این موضوع در متون واقعی که عموما بزرگتر نیز هستند ، مشهودتر است . همان طور که قبلا بیان شد ، این از ویژگی های آماری زبان های طبیعی است و این مسئله به ما نشان می دهد که این متن توسط رمزنگاری جانشینی رمز شده است . زیرا در این روش رمزنگاری ، شکل حروف عوض نمی شود و فقط جای آنها تغییر می کند .

دانشجویان محترم:

جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.

منابع فارسی :

[۱] اندرو تننن بام, مترجمان حسین پدرام, علیرضا زارع پور, احسان ملکیان , شبکه های کامپیوتری ,چاپ پنجم, تهران, نص, ۱۳۸۴

[۱۱] الگوریتم RSA

Http://amath.blogfa.com/post-۵۲.aspx

[۲۰] بهداری,م., سلماسی زاده, م., مهاجری,ج., معماری امنیتی سیستم تلفن همراه نسل دوم (GSM) و آسیب پذیری آن, فصلنامه علمی و پژوهشی شریف, شماره سی و ششم, ص, ۳۱-۴۱, تابستان ۱۳۸۶

منابع انگلیسی:

[۲] David Crawford / Mike Esterl, At Siemens, witnesses cite pattern of bribery, The Wall Street Journal, January ۳۱rd, ۲۰۰۷

[۳] Karen Hunter, "Quantum Cryptography" , ۲۰۰۲

[۴] Quantum cryptography

http://en.wikipedia.org/wiki/Quantum_cryptography

[۵] Code for 'Unbreakable' Quantum Encryption Generated at Record Speed over Fiber

http://www.physorg.com/news۶۴۵۸۹۵۳۹.html

[۶] Record key speed set by fiber QKD system at NIST

http://www.nist.gov/itl/quantum/recordkey.cfm

[۷] Data Encryption Standard

http://en.wikipedia.org/wiki/Data_Encryption_Standard

[۸] DATA ENCRYPTION STANDARD (DES)

http://www.itl.nist.gov/fipspubs/fip۴۶-۲.htm

[۹] Advanced Encryption Standard

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[۱۰] RSA

http://en.wikipedia.org/wiki/RSA

[۱۲] MD۵

http://en.wikipedia.org/wiki/MD۵

[۱۳] ۲Tao Xie, ۱Dengguo Feng, "How To Find Weak Input Di®erences For MD۵ Collision Attacks", ۲۰۰۹

[۱۴] Public key infrastructure

http://en.wikipedia.org/wiki/Public_key_infrastructure

[۱۵] Kerberos: An Authentication Service for Computer Networks

http://gost.isi.edu/publications/kerberos-neuman-tso.html

[۱۶] Global System for Mobile Communication (GSM), The International Engineering Consensus, http://www.iec.org.

[۱۷] C. Peng, GSM and GPRS Security, Telecommunication Software and Multimedia Laboratory, Helsinki University of Technology,۲۰۰۰

[۱۸] J. Alfred, C. Paulvan Oorschot, "Hand Book of Applied Cryptographic", ۱۹۹۶

[۱۹] H. Federrath, "Protection in Mobile Communications", Dresden University of Technology, Department of Computer Science, D-۰۱۰۶۲ Dresden, Germany, ۱۹۹۹