

زنجان دانشکده هنری کروه برق آزمایشگاه پژوهش و انتشاره زنجان دانشکده هنری کروه برق آزمایشگاه پژوهش و انتشاره زنجان دانشکده هنری کروه برق آزمایشگاه پژوهش و انتشاره زنجان

و اشکده هندسی کروه برق آزمایشگاه پروره برق و اشکده زنجان و اشکده هندسی کروه برق آزمایشگاه پروره برق و اشکده زنجان و اشکده

مہندسی کروہ برق آئینا گاہ پرورہ برق و انسٹکھا زنجان و اسکدہ مہندسی کروہ برق آئینا گاہ پرورہ برق و انسٹکھا زنجان و اسکدہ مہندسی

# دانشکده مهندسی کروه برق آذربایجان و ائمداد زنجان

## پروژه های ایجاد پرورش برق و اسکله زنجان

## پایان نامه کارشناسی

برن و داکله رجحان و داکله همندی رووه برن ارمایکاهه پوره برن داکله رجحان و داکله همندی رووه برن ارمایکاهه پوره برن

۱۵ داده هستند که تا سیزدهم آذر ماه این سرمه را در خانه نداشته باشند.

کوئی نہیں کر سکتے کہ وہی پسپورٹ

استاد راهنمای: دکتر مسعود شفیعی

جناب آقای دکتر محمدی

سرق و انشاه زنجان و اشکده همند سی کروهه رق آزمايگاهه روزهه رق و انشاه زنجان و اشکده همند سی کروهه رق آزمايگاهه روزهه رق

دانشگاه زنجان و اشکده هنری کروهه برق و اندیشه هنری رودوز آزادی کارهای هنری بر ق رفق و اندیشه هنری کروهه بر ق آزادی کارهای هنری بر ق و اندیشه

**زنجان و آشکده هندی فهرست:** آگاه پروژه برق و انشا زنجان و آشکده هندی کروه برق آزما گاه پروژه برق و انشا زنجان و آشکده هندی کروه برق آزما گاه پروژه برق و انشا زنجان

<sup>۳</sup> فصل اول ..... و اشکده مهندسی کروهه بین آرایه کاهه بورهه سی و اشکده ریحان و اشکده مهندسی کروهه بین آرایه کاهه بورهه سی و اشکده ریحان و اشکده مهندسی کروهه بین آرایه کاهه بورهه سی و اشکده ریحان و اشکده مهندسی کروهه بین آرایه کاهه بورهه سی و اشکده ریحان و اشکده

#### ۱- تاریخچه رمزنگاری

## ۱- مقدمه ای بر رمزنگاری ۲- مقدمه ای بر رمزنگاری

### ۱-۳- رمزگاری جانشینی

برق آزمایشگاه پژوهشی زنجان و اسکله زنجان دارند. همچنان که در پژوهش آزمایشگاه پژوهشی زنجان و اسکله زنجان داشتند، این اسکله هم‌نیز کروه برق را نیز می‌گردانند.

۱-۵-۵- رمزپردازی بر مبنای به هم ریختنی محتوای پیام ..... ۱۱

#### ۱-۶ - رمزنگاری کوانتومی

فصل دوم ..... ۲۴

۲-۱- **الگوریتم های رمزگاری با کلید متقاضان** ۲۴

**۲-۲- رمزنگاری DES** (استاندارد رمزنگاری اطلاعات) ۲۵

<sup>۳</sup>-۲- روش سفید سازی در الگوریتم DES

۲-۴- منیگای DES سه گانه

Digitized by srujanika@gmail.com

**ا-۷- رمزگاری (rijndael)** ریجندل یک الگوریتم پردازش داده است که در سال ۱۹۹۷ معرفی شد و در همان سال انتخاب شد تا به عنوان استاندارد رمزگاری داده های پردازشی برروز رود.

برق آزمایشگاه پژوهشی و تحقیقاتی آزاده پژوهی و آزاده زنگنه و آزاده هندسی کرومه بریت ۳۵-۶-الگوریتم های کلید عمومی

**فصل سوم :** آنکاہ روحانی و اسلامی تحریر اور درود اسلامی کو اپنے روحانی و اسلامی تحریر اور درود اسلامی کو اپنے

### ۱-۳- امضاهای دیجیتالی

### **۴-۲- امضاهای دیجیتالی با کلید متقارن ..... ۴۰**

<sup>۴۱</sup>- ۳- امضاهاء، دیجیتال، با کلید عمومی.

۱-۱- امصاری دیجیتالی با استفاده از حلاصه پیام زنگان و اشکده مهندسی کرومه رق آذنایگاه روزه رق و اشکده زنگان و اشکده مهندسی کرومه رق آذنایگاه روزه رق و اشکده زنگان

زنگان و اشکوه منطقه‌ای کوچک است اما در آن سه روستا که هر کدام دارای یک مدرسه ابتدایی هستند، از این مدارسی که در روستاها قرار دارند، دو تا در اشکوه و یک تا در زنگان و این مدارسی که در روستاها قرار دارند، دو تا در اشکوه و یک تا در زنگان

**فصل چهارم** وانگاهه ریحان والکلهه مهندسی کروورن آرایاگاهه ریورهه بن وانگاهه ریحان والکلهه مهندسی کروورن آرایاگاهه ریورهه بن وانگاهه ریحان والکلهه مهندسی

**۴- مدیریت کلیدهای عمومی** ۴۹  
کروه برق آنالایکاوه روزمرن و اسکاوه زجان و اسکده هندی روزمرن آنالایکاوه روزمرن و اسکو زجان و اسکده هندی کروه

**فصل پنجم** ..... ۵۶  
رق آزیاگاه رودهرق و اسکله زیان و اسکله هندسی روهر آذن کارهه رودهرق اسکله زیان و اسکله هندسی لعوهر آزیاگاه رودهرق و اسکله هندسی کروهه رق

## ۲-۵- احراز هویت بر مبنای کلید مشترک

### ۳-۵ احراز هویت توسط مرکز توزیع کلید (KDC)

۴- پروتکل احراز هویت نیدهام - شرودر ..... ۵

۵-۵- پروتکل احراز هویت اتوی - ریس

۵-۶-روش احراز هویت در ویندوز ۲۰۰۰

۵- احراز هویت با استفاده از رمزنگاری با کلید عمومی

سندی کوہاٹ، اقصیٰ سیم : ۱۲ جنوری ۲۰۰۶ء

امنیت در شبکه GSM

برنامه های آموزشی و پژوهشی موسسه علمی پژوهشی اسلامی

از نایابه پروره بین و امکانات احتمالی داشته باشند که در اینجا آنها را در پیشنهاد می‌نماییم.

برق و اسکاہ زنجان و اسکده هندسی کروه برق آزمایگاه پروره برق دالکاه رجحان و اسکده هندسی کروه برق آزمایگاه پروره برق

۶-۷- افشه همیزه مکان مشتک

زنگان و اشکده مندوی را می‌توان بازیابی کلید Ki با دسترسی فیزیکی به SIM کارت این سه شهر پسرخان، زنگان و اشکده مندوی را بروز رساند.

۶-۹- بازیابی کلید Ki بدون دسترسی فیزیکی به SIM و از طریق فاصله هواپی ...  
دانشکده هندی کوهنوردی از راهنمایی کوهنوردی و آنچه زبان دانشکده

۶-۱- عدم سرویس دهنده (DoS) محدودی که در برخی آنلاین کارهای روزمره مانند خرید و پرداخت از طریق بانک و انتشار رسانی می‌گذارد.

٦-١١- حمله به الگوريتم A5

منابع فارسی ..... ۸۹

منابع انگلیسی،  
..... ۹ .....

**فصل اول** انشاہ زنجان و آنکدہ مہندسی کروہرمنق آنماگاہ بروہرمنق دانشاہ زنجان و آنکدہ مہندسی کروہرمنق آنماگاہ بروہرمنق دانشاہ زنجان و آنکدہ مہندسی

کروه برق آزما یاگاه و انشا زنجان کروه برق آزما یاگاه و انشا زنجان داشکده ۱- تاریخچه رمزنگاری:

کلمه رمزگاری<sup>۱</sup> از لغتی یونانی به معنای محرمانه نوشتن متون برداشت شده و

آزمایشگاه پژوهشی پیشینه ای طولانی دارد. از نظر تاریخی نظامیان، هیات های سیاسی، خاطره کروهی می باشد.

روزهای آنچه اتفاق آیده روزه نویسان و عشاق از رمزگاری بیشتر استفاده کرده و در گسترش آن نقش

برن دانش و زبان بیشتری داشته اند ولی نقش نظامیان پر رنگ تر بوده است. تا قبل از ابداع

دانشگاه زنجان و اکادمی علوم پژوهی هنر و اندیشه کامپیوتر پیامدها توسط یک کارمند رمز و ارسال می شدند. و این روش

**مشکلاتی داشت. از قبیل:** زنجان و آذربایجان را در پیش از آنها می‌گذاشتند و آنها را بزرگ کردند.

۲. محدودیت در تغییر روش رمزگاری به دلیل نیاز مجدد به آموزش افراد حرفه‌ای که روش آزمایشگاهی را در زبان و اسلکه مهندسی که در هر آزمایشگاه روشی متفاوت داشته باشند، می‌توانند این روش را در آزمایشگاه خود آزمایش کنند.

۴. فاش شدن روش رمزگاری در صورت دستگیری افراد مطلع از آن که درین آئینه کاهروهه مرق و اشکه و هندسی کوچوت آئن کاهروهه مرق و اشکه و زخان و اشکه و هندسی لر و هر ق آئنایگاهه روزهه مرق و اشکه و زخان و اشکه و هندسی کروه

از زیگاوه روهرق وانگه زخار و آنکه همین سو که روهرق است از زیگاوه روهرق وانگه زخار و آنکه همین سو که روهرق است از زیگاوه روهرق وانگه زخار و آنکه همین سو که روهرق است

بچوں کی بھروسہ اور اپنے بھائیوں کی بھروسہ، اسکے لئے اپنے بھائیوں کی بھروسہ، اسکے لئے اپنے بھائیوں کی بھروسہ۔

---

1. Cryptography

هندي کروهه هر ق آنرا در نظر گرفت : زنجان و اشكده هندسي کروهه هر ق آنرا گاهه بروزه هر ق دانشاه زنجان و اشكده هندسي کروهه هر ق آنرا گاهه بروزه هر ق دانشاه زنجان و اشكده هندسي

<sup>۱</sup>. متن آشکار<sup>۱</sup> : پیامی است که می خواهیم آن را رمزگاری کنیم (P) که در آن آذایش و مرگ و ازایش و زخم و ایجاد مصدومیت را در اینجا می خواهیم تصور کرد.

۲. کلید<sup>۲</sup>: پارامتر تابع رمزنگاری (K)

۳. متن رمز<sup>۳</sup> : نتیجه عملیات رمزگاری (C)

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

$$C = E_k(P)$$

دانشگاه زنجان و اکادمی کوچرق آزادگان، دانشگاه زنجان و اکادمی کوچرق آزادگان، دانشگاه زنجان و اکادمی کوچرق آزادگان،  
معنای این تابع این است که  $R$ -منگاری بر روی متن آشکار  $P$  و توسط تابع  $E$  با

با امت K انجام شده است و متن از C بدست آمده است.

اگر بتوان معکوس تابع رمزگاری را بدست آورد، قادر به یافتن متن آشکار

جهتی کروه برق آخوهیم شد. و انشکاه زنجان و اشکده همدی کروه برق آزما یگاهه ریوژه برق و انشکاه زنجان و اشکده همدی کروه برق آزما یگاهه ریوژه برق و انشکاه زنجان و اشکده همدی

$P = D_k(E_k(P))$  که می‌گویند از یک آنلاین کاوه روزه برق و اسکده زنجان داشته باشید و ممکن است کروه برق آنلاین کاوه روزه برق و اسکده زنجان داشته باشید و ممکن است کروه

برن آذایشگاه و پروره از آنجایی که محرومانه نگه داشتن روش رمزنگاری خیلی مشکل است، به عنوان متدی کروهی

یکی از قواعد اساسی در رمزگاری، شخص رمزگار باید این فرض را پذیرد که آزمایشگاه روزمره ممکن است محتویات آزمایش را در خود نگیرد.

همه افراد روش رمزنگاری یعنی تابع E و روش رمزگشایی یعنی تابع D را می‌آزمایند که بروزگیری آنها را بسیار سخت کرده است.

بروزه برق و انتگاره زنجان و اشکده هندسی لروده برق را با توجه به این دو انتگاره برق و اشکاده هندسی کروهه برق آذایگاهه برجهات و اشکاده زنجان و اشکاده هندسی کروهه برق آذایگاهه برجهات دانند و تنها کلید رمز **k** پنهان است.

زنجان و اشکده همندی کروهه برق آذنایگاه روزهه برق و اشگاه زنجان و اشکده همندی کروهه برق آذنایگاه روزهه برق و اشگاه زنجان و اشکده همندی کروهه برق آذنایگاه روزهه برق و اشگاه زنجان

پژوهشی ریز آنلاین و انتگاری روش برای انتخاب زمان و انتگاره مدنی کروهه برق آنلاین کاهه بروهه برق آنلاین کاهه بروهه  
با توجه به آشکار بودن الگوریتم رمزنگاری، تضمین غیرقابل شکسته بودن یک  
برق و انتگاره زمان و انتگاره مدنی کروهه برق آنلاین کاهه بروهه برق آنلاین کاهه بروهه برق و انتگاره زمان و انتگاره مدنی کروهه برق آنلاین کاهه بروهه برق  
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 چانشپنی:

پروژه برق و انرژی هرچند برای رمز شکنی متون رمز شده به این روش باید حالت آتیاگاه پروژه !

برق و انتگاه زنجان مختلف در نظر گرفته شود، اما متخصصان رمز شکنی، برای گشودن این رموز از آنها گام پروردگاری می‌کنند.

روش هوشمندانه‌ی دیگری که وی می‌تواند اتخاذ کند، حدس زدن یک کلمهٔ هنری که در یک متن است. به عنوان مثال فرض کنید که یک متن رمز شده که مربوط به ایران است به شخصی داده شده است. وی حدس می‌زند که کلمهٔ هنری که در آن متن وجود دارد.

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

با توجه به دو مورد بالا، می‌توان یافت که کلمه IRANIAN در جایگاه ۳۹ صندی کرومه آنلاین و در مجموع داشتاری را در محدوده منطقه ای از شهر رجستان و شهر روحان و شهر رجستان و شهر روحان داشته باشد.

۱-۴- رمزگاری جایگشتی: تراشکار و مرتع زنجان و اردبیل هندسی کروهمن تراشکار و مرتع زنجان و اردبیل هندسی کروهمن

آراییگاه روزه‌من در این روش، جای حروف عوض می‌شود و لی شکل آنها تغییر نمی‌کند. برای کوچه‌من آنها گاه

روزه رق و انتگاه زنجان و اشکده مهندسی کروه رق آذربایجان غربی

مرق و انجکاه زنخان (۱) انتخاب کلید رمز مرق و انجکاه زنخان و اسکدہ مهندسی کروه مرق آزمایشگاه روزه مرق

۲) شماره گذاری ستون ها براساس تقدم الفبایی حروف کلید رمز و انتها زنجان و آنکه همچنان آنرا یافته باشیم.

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

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

روش بالایک روشنگری و عمومی برای رمزگاری به صورت جایگشتی است و

برای توضیح بیشتر، مثال زیر را در نظر می‌گیریم.

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

**آزمایشگاه پژوهشی و انتشارات علمی اسلامی** مهندسی کروپونق آزمایشگاه پژوهشی و انتشارات زبان و اندکه مهندسی کروپونق

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

پژوهشی از زبان و ادبیات اسلامی را در میان آنها بررسی کرد. آنها پژوهشی از زبان و ادبیات اسلامی کردند. آنها پژوهشی از زبان و ادبیات اسلامی کردند.

برق و انجام زنگان و اسکده هندسی کروهه برق آزمایشگاه پژوهه برق و انجام زنگان و اسکده هندسی کروهه برق آزمایشگاه پژوهه برق و انجام زنگان و اسکده هندسی کروهه برق آزمایشگاه پژوهه برق

حال با استفاده از کلید رمز فوق، یک ماتریس شامل ۸ ستون تشکیل می‌دهید

و بعد متن آشکار را در زیر آن به صورت افقی می نویسیم .

ي	و	و	ر	ن	ا	م	ه
ل	د	ي	خ	ف	ي	ز	ز
و	ه	ي	ن	س	ي	ن	س
ي	ت	س	س	ت	ا	ر	ت
ا	ت	ت	ا	ك	ك	و	ي
ت	ه	ا	ل	ل	پ	و	و
ي	ر	ا	ب	ك	د	ي	ف

حال بر اساسی، ترتیب هر سهون، متن داشته باشد، نویسی:

حال برآسنس تریب هر سیوون، من رمر سده را می نویسیم.

uakpdstiwfnrwoestcLchtthrnSaLbestaaeweate

پروژه برق و انشاگاه زنجان و انشاگاه معدنی کروه برق آذنیاگاه پروژه برق و انشاگاه زنجان و انشاگاه معدنی کروه برق آذنیاگاه پروژه است و فقط جای آنها در متن عوض شده.

برق و انجام زیبایی کارهای پرورشی

دانشگاه زنجان و دانشگاه آزاد اسلامی پرورشی زنجان و دانشگاه آزاد اسلامی کروه برق آزادگان و پرورشی زنجان و دانشگاه

زبان و اشکده مدنی) حصول اطمینان از اینکه این متن توسط رمزنگاری جایگشتی رمز شده باشد.

۲) تشخیص تعداد ستون ها

۳) بدست آوردن ترتیب ستون ها

۱. اگر متن رمز شده را بررسی کنید خواهید یافت که حروف t, e, a, و .

در متن زیاد تکرار شده اند و این موضوع در متون واقعی که عموماً بزرگتر آنها گاه روزمرق و آنها گاه روزمرق آنها گاه روزمرق

نیز هستند، مشهودتر است. همان طور که قبلابیان شد، این از ویژگی

های آماری زبان های طبیعی است و این مسئله به مانشان می دهد که این

متن توسط رمزگاری جانشینی رمز شده است. زیرا در این روش رمزگاری

، 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 پژوهش گروه برق مراجعه فرمایید.

**منابع فارسی:** برق و انتشاره زنجان و اکنده هندی کروه برق آزنا یاگاه پروره برق و انتشاره زنجان و اکنده هندی کروه برق آزنا یاگاه پروره برق و انتشاره زنجان

[۱] اندر و تئن بام، مترجمان حسین پدرام، علیرضا زارع پور، دانشکده هنری

احسن از این کار این شکوه و ای که این مقتدرانه از این دنیا نمیگذرد

رسانی و اسلام‌گردانی لرستان

[Http://amath.blogfa.com/post-۸۲.aspx](http://amath.blogfa.com/post-۸۲.aspx)

[۲۰] به داری دم، سلاماسی زاده، م.، مهاجری رج.، معماری امنیتی

زنگان و اسلام شهری که سیستم تلفن همراه نسل دوم (GSM) و آسیب پذیری آن را در زنجان

دانشگاه علوم پزشکی کوهدشت فصلنامه علمی دانشگاه علوم پزشکی کوهدشت انتشارات دانشگاه علوم پزشکی کوهدشت

**زنجان و اشکده هند منابع انگلیسی:** بنی دانشگاه زنجان و اشکده هندی کروه برق آزماییگاه پژوهه برق دانشگاه زنجان و اشکده هندی کروه برق آزماییگاه پژوهه برق دانشگاه زنجان

[۷] David Crawford / Mike Esterl, At Siemens, witnesses cite pattern

کروهون آزمایش روش دری و انجام زمانی واکنش می‌گیرند و این روش ممکن است که

[۳] Karen Hunter, "Quantum Cryptography", ۲۰۰۲، [دانشگاه زیخان و انجمن علمی](#)، آنلاین معرفی کرد.

[http://en.wikipedia.org/wiki/Quantum\\_cryptography](http://en.wikipedia.org/wiki/Quantum_cryptography)

[A Code for "Unsupervised Quantum Execution Generated at Random"]

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

<http://www.physorg.com/news/100411.html>

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

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

## [v] Data Encryption Standard

[http://en.wikipedia.org/wiki/Data\\_Encryption\\_Standard](http://en.wikipedia.org/wiki/Data_Encryption_Standard)

## [۸] DATA ENCRYPTION STANDARD (DES)

<http://www.itl.nist.gov/fipspubs/fipspub.htm>

برق دا شکاہ زنجان و اسلامکه همندی کروه برق آزمایگاه پروژه برق دا شکاہ زنجان و اسلامکه همندی روپرینه اړیکه پروژه برق

دانش و زبان دانشجویی کنونی و آینده [http://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)



