بسم الله الرحمن الرحيم

دانشگاه هرمزگان

دانشکده علوم پایه

گروه ریاضی

**پایان نامه تحصیلی برای دریافت درجه کارشناسی ارشد**
**رشته ریاضی محض – گرایش جبر**

# عنوان:
# نظریه اعداد و رمزنگاری

**استاد راهنما:**
**دکتر مرضیه قائدی**

**نگارش:**
**کاوه گودرزی**

**خرداد ۱۳۹۰**

## چکیده

رمزنگاری در واقع مطالعه روشهای ارسال و دریافت پیامهای رمزی است. در حالت کلی فرستنده های است که سعی می کند پیام را به گیرنده ارسال کند و دشمنی که می خواهد پیام را به رباید. فرستنده در صورتی موفق است که بتواند پیام را برباید. فرستنده در صورتی موفق است که بتواند پیام را به گیرنده ارسال کند بدون اینکه دشمن بفهمد که پیام چه بوده است.

البته شکستن رمز بوسیله دشمن کار مشکلی است. اگر کتاب رمز منتشر شود دشمن می تواند آن را در اختیار داشته باشد و بدون استفاده ار ریاضیات پیشرفته قادر به شکستن کد نخواهد بود.

در این پایان نامه سعی شده است که با استفاده از نظریه اعداد و روشهای رمزنگاری راههای مختلفی برای رمزنگاری راههای مختلفی برای رمزی کردن یک متن ارایه شود. در فصل ۲ قضایا و تعاریفی از نظریه اعداد که مورد استفاده در رمزنگاری است داده شده است. در فصل ۳ الگوریتم های جهت سریعتر محاسبه کردن ضرب چندجمله ایها و در فصلهای ۴ تا ۱۰ چندین الگوریتم در مورد رمزنگاری مورد توجه قرار گرفته است.

تقدیم به:

پدر و مادر دلسوز

و

همسر مهربان و فرزند دلبندم

# تشکر و قدردانی:

سپاس خدایی راکه نیکوهای آفرینش را برای ما برگزید.

و سپاس مخصوص خدای مهربانی که به انسان توانایی و دانایی بخشید تا بندگانش شفقت ورزد، مهربانی کند و در حل مشکلاتشان یاری شان نماید. از راحت خویش بگذرد و آسایش هم نوعان را مقدم دارد، با او معامله کند و در این خلوص انباز نگیرد و خوش باشد که پرودگار سمیع و بصیر است.

بدینوسیله از زحمات اساتید گرامی سرکار خانم دکتر مرضیه قائدی که راهنمایی این پژوهش را بر عهده داشتند تشکر و قدردانی می نمایم. از جناب آقای دکتر مهدی سبزواری که زحمت مشاوره این پایان نامه را بر عهده داشتند بی نهایت سپاسگزارم. در نهایت از زحمات سرکار خانم مهندس اعظم قائدی و خانم محمدی کمال تشکر را داریم.

## فهرست مطالب

### فصل اول: مقدمه



### فصل دوم: نظریه اعداد

**فصل سوم: چند الگوریتم و تبدیل**



**فصل چهارم: رمز نگاری**

**فصل پنجم: تابع یک طرفه H**



**فصل ششم: توابع و رمز های خطی آفین**



**فصل هفتم: سیستم های رمز گذاری**



**فصل هشتم: الگوریتم DES**

# فصل اول

## مقدمه

## ۱-۱- تئوری اعداد چیست؟

طرح این سوال انگیزه تلاش اولیه در ارائه یک تعریف است.تئوری اعداد عبارت است از مطالعه مجموعه اعداد صحیح یا برخی از زیر مجموعه های آن یا مجموعه هایی شامل آن.با این فرض که اعداد صحیح به تنهایی و نسبت به یکدیگر بدون توجه به نقش آنها در اندازه گیری جالبند.ظاهرا دامنه این تعریف حساب مقدماتی را شامل میشود. مروری گذرا بر خواص مقدماتی اعداد صحیح در بخش ۱ از فصل دوم آمده است.یکی از مفاهیم بنیادی تئوری اعداد اعداد اول هست. عدد صحیح p اول است اگر $p \neq \pm 1$ و معادله p=ab جوابی بغیر از $a = \pm 1$ یا $a = \pm p$ نداشته باشد. بنابراین به اختصار میتوان گفت که عدد اول عدد صحیحی است که مخالف $\pm 1$ باشد و هیچ مقسوم علیه نابدیهی نداشته باشد.

## ۱-۲- تاریخ نخستینِ تئوری اعداد

تمدن بین النهرینی نخستین تمدنی است که اسناد موجود از فعالیتهای ریاضی در آن دوره حکایت میکند.تقویمهایی وجود دارد که تاریخ شروع این دوره را ۲۱۰۰ قبل از میلاد معین میکند ونشان از درک سومریها از اندازه گیری توپولوژیکی و حل بعضی معادلات مربعی و استفاده از اعداد منفی دارد. اولین نشان متقاعد کننده که دانشمندان باستان شناس از تئوری اعداد یافتند در سال ۱۹۴۵ کشف شد.و آن هنگامی بود که ا.نگیور[۱] و ا.ساخز[۲] لوح مشهور به پلیمپتون[۳] ۳۲۲ را از دانشگاه کلمبیا مورد تحلیل قرار دادند.از زبانی که در آن بکار رفته میتوان تاریخ آن را 1900 الی 1600 قبل از میلاد نزدیک اولین سلسله بابلی و هزار سال قبل از مدرسه فیثاغورث استنباط کرد.از میان سه ریاضیدان برجسته که عصر طلایی ریاضیات یونان را پدید آوردند(اقلیدس-آپولونیوس-ارشمیدس) تنها اقلیدس است که به نظر میرسد کار زیادی در تئوری اعداد کرده باشد.

---

1. Alen Ngiver
2. A. sakhez
3. Pelempton University

با زوال نفوذ یونانیان و ظهور امپراطوری رم مرکز تمدن در قرن هجدهم به بغداد انتقال یافت. از نقطه نظر امروزی سهم اصلی را ریاضیدانان عرب در اقتباس سیستم اعداد هندی, جبر اعداد اصم و نگهداری ریاضیات قدیم یونان دارند.پس از گذشت چند ین سال بیداری اروپا آغاز گشت جنبشی علمی در اروپا شکل گرفت و در مدت ۵۰ سال بیش از ۳۰۰۰۰ نسخه از کارهای علمی شامل ریاضیات قدیم, به یونانی, لاتین وعربی منتشر شد. نظریه اعداد امروزی از همان زمان شروع گردید.

## ۳-۱- استفاده از تئوری اعداد در رمز نگاری

رمزنگاری مطالعه روشهای ارسال و دریافت پیامهای محرمانه است.در طول شش هزار سال تا زمانیکه راهنمای عمومی در سال ۱۹۷۰ میلادی اختراع شد ریاضیاتی که در رمزنگاری استفاده می شد زیاد جالب نبود. در قرن بیستم رمزنگارها استفاده کمی آنهم از بعضی مفاهیم که در حاشیه ریاضیات بود میکردند. البته در آن زمان استثنائاتی وجود داشت در سال ۱۹۴۰ میلادی ا. تورینگ[1] پدر علم کامپیوتر مفاهیم گسترده ای را در رمزنگاری به کار بردکه از آن جمله استفاده از تکنیکهای آماری برای شکستن یک کد بود. همچنین ک.شانون[2] در مورد بنیان رمزنگاری اقداماتی انجام داد.

---

1. Alan Turing
2. Claude Shannon

در همان دهه ج.هاردی [1] طی مطلبی در توجیه ریاضیدانان نوشت: "شاید شادمانی ریاضیدانانی چون گاوس[2] و لیزر[3] موجه بود که می گفتند تنها یک علم (نظریه اعداد) در هر رشته وجود دارد."

این تصور از نظریه اعداد تنفر عمیقی را بر جا گذاشت. در سال ۱۹۷۷ میلادی سه دانشمند علوم کامپیوتر از دانشگاه تکنولوژی ماساچوست به نامهای ریوست و شامیر و یان [5] یک روش جدید در سیستم رمزنگاری بوجود آوردند که آنرا سیستم RSA نامیدند.

در سال ۱۹۸۴ میلادی هنریک [4] مطالبی را پخش کرد که در آن یک روش جدید بر اساس اعداد صحیح بزرگ که در منحنیهای بیضوی استفاده می شد توضیح داده شده بود.اخیرا با ظهور اینترنت و تجارت الکترونیک رمزنگاری برای اقتصاد جهانی و میلیونها انسان که در کارهای روزانه- شان از آن استفاده می کنند ضروری شده است.اطلاعات حساسی مانند حسابهای بانکی و کارتهای اعتباری یا مبادلات شخصی هر کدام بصورتی به رمزنگاری ارتباط دارند بطوریکه فقط خود شخص بتواند از این خدمات استفاده کند.

---

1. G.H.Hardy

2. Gauss

3. Lesser

4. Hendrik Lenstra

5. Ron Rivest - Adi Shamir - Ien Adleman

# فصل دوم

# نظریه اعداد

### ۱-۲- الگوریتمهای بنیادی اعداد

برای شروع به تعدادی از قوانین نظریه اعداد مقدماتی شامل تعدادی علائم و تعاریف احتیاج داریم. فرض کنید b,a دو عدد صحیح مثبت باشند نماد a|b بیان می‌کند که a یک شمارنده b است یا b بر a بخش پذیر است. اگر a|b در اینصورت عدد صحیح k موجود است بطوریکه b=ak . خواص زیراز تعریف بالا نتیجه می‌شود:

**قضیه**(۱-۱-۲): فرض کنید $a, b, c \in z$ اعداد صحیح دلخواهی باشند در اینصورت:

الف) اگر b|c , a|b آنگاه a|c .

ب ) اگر a|c , a|b آنگاه:

$$\forall a, b \epsilon Z \quad ; \quad a|bi + c$$

ج ) اگر b|a , a|b آنگاه a=±b.

**تعریف**(۲-۱-۲):عدد صحیح p رااول گوئیم هر گاه:

(i) $P \geq 2$

(ii) تنها شمارنده‌های آن اعداد p , 1 باشند. بنابراین در حالتی که P عدد اولی باشد و d|p آنگاه $d = 1$ یا $d = P$

- عدد صحیح بزرگتر از ۲ را که اول نباشد مرکب گوئیم.

**قضیه بنیادی حساب** (۳-۱-۲): اگر $n \succ 1$ عدد صحیحی باشد بنابراین مجموعه منحصر بفرد از اعداد اول $\{P_1, P_2, \ldots P_k\}$ موجودندبطوریکه $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ جائیکه $e_i$ها اعداد صحیح مثبت هستند.

## ۲-۲- بزرگترین مقسوم علیه مشترک (GCD)

**تعریف**(۱-۲-۲): بزرگترین مقسوم علیه مشترک دو عدد صحیح مثبت a,b که با نماد $\gcd(a,b)$ نمایش داده می‌شود بزرگترین عدد صحیحی است که $a,b$ را بشمارد و اگر $d \in z$ موجود باشد بطوریکه $d|a \,, d|b$ آنگاه $d|\gcd(a,b)$.

**تعریف** (۲-۲-۲): اگر $\gcd(a,b) = 1$ در اینصورت می گوئیم $a,b$ نسبت به هم اولند.

- $\gcd(a,0) = a$
- $\gcd(a,b) = \gcd(|a|,|b|)$

## ۳-۲- عملگر مدولی mod

باقیمانده تقسیم a بر n را با a modn نمایش میدهیم که بصورت $r = \text{a modn}$ می‌باشد. این بدان معنی است که :

$$r = a - \left[\frac{a}{n}\right] n$$

به عبارت دیگر برای اعداد صحیح مانند q داریم:

$$a = nq + r \quad ; \quad 0 \le r < n$$

توجه به این نکته لازم است که amodn همیشه یک عدد صحیح از مجموعه $\{0,1,\dots,n-1\}$ می‌باشد حتی اگر a منفی باشد. گاهی اوقات به عملگر mod همنهشتی گفته می‌شود.

**تعریف** (۱-۳-۲): اگر a modn= b modn باشد می گوئیم a,b به پیمانه n همنهشت هستند و می‌نویسیم $a \equiv b \pmod n$

- اگر $a \equiv b \pmod n$ آنگاه

$$a - b = nk \quad ; \quad k \epsilon z$$

## ٤-٢- رابطه بین عملگر مدولی و GCD

قضیه زیر توصیف دیگری از بزرگترین مقسوم علیه مشترک به ما می‌دهد که به وسیله عملگر مدولی اثبات می‌شود.

**قضیه**(۱-۴-۲):برای اعداد صحیح و مثبت a,b  $\gcd(a,b)$ کوچکترین عدد صحیح مثبت d است بطوریکه $i,j\epsilon z$ ; $d = ai + bj$ به عبارت دیگر اگر d کوچکترین ترکیب خطی صحیح مثبت از a,b باشد آنگاه $d = \gcd(a,b)$ .

اثبات: فرض می‌کنیم d کوچکترین عدد صحیح مثبتی است که $d = ai + bj$ برای بعضی $i, j \in z$ از تعریف d نتیجه می‌شود که هر شمارنده مشترک a,b عدد صحیح d را نیز می‌شمارد بنابراین $d \geq \gcd(a,b)$. حال باید نشان دهیم $d \leq \gcd(a,b)$ . فرض کنید $h = \left[\frac{a}{d}\right]$ بطوریکه h عدد صحیحی است که:

$$a \bmod d = a - hd$$

بنابراین

$$\begin{aligned} a \, mod d &= a - hd \\ &= a - h(ai + bj) \\ &= (1 - hi)a + (-hj)b \end{aligned}$$

به عبارت دیگر amodd نیز ترکیب خطی از a,b است با توجه به تعریف عملگر مدولی $a \bmod d < d$ اما d کوچکترین ترکیب خطی صحیح مثبت از a,b است. بنابراین باید نتیجه بگیریم amodd=0 و این نشان می‌دهد که $d \mid a$ . همچنین با استدلالی مشابه میتوان نتیجه گرفت که $d \mid b$. پس d یک شمارنده مشترک a,b است که نشان می‌دهد $d \leq \gcd(a,b)$

همانطور که بعداً خواهیم دید این قضیه برای محاسبه معکوس ضربی مدولی اعداد مفید است.

## ۵-۲-الگوریتم اقلیدسی برای محاسبه gcd

برای محاسبه $gcd$ دو عدد میتوان از یکی از قدیمترین الگوریتمها بنام الگوریتم اقلیدسی استفاده کرد.

این الگوریتم بر پایه خواص $\gcd(a,b)$ می‌باشد.

**لم**(۱-۵-۲): فرض کنید a,b دو عدد صحیح مثبت باشند در اینصورت برای هر عدد صحیح $r \in z$ داریم:

$$\gcd(a,b) = \gcd(b, a-rb)$$

اثبات: فرض کنید

$$C = \gcd(b, a-rb), d = \gcd(a,b)$$

بطوریکه d بزرگترین عدد صحیحی است که $d \mid a \quad , \quad d \mid b$ و c نیز بزرگترین عدد صحیحی است که $c \mid b \quad , \quad C \mid a-rb$ باید ثابت کنیم d=c. طبق تعریف d عدد

$$\frac{a-rb}{d} = \frac{a}{d} - r\left(\frac{b}{d}\right)$$

یک عدد صحیحی است. پس d یک شمارنده $a-rb$ است پس $d \le c$.

طبق تعریف c عدد $k = \frac{b}{c}$ نیز باید یک عدد صحیح باشد زیرا $c \mid b$ بنابراین $\frac{a-rb}{c} = \frac{a}{c} - r\left(\frac{b}{c}\right)$ نیز یک عدد صحیح است. پس نتیجه می گیریم c|a پس c هم a و هم bرا می‌شمارد و $c \ge d$ بنابراین $c = d$.

$A\lg orthm\ Euclid\ GCD\ (a,b);$

$input: \quad a,b \in z^{+} U \{0\}$

$output: \gcd(a,b)$

$if\ \ b = 0 then$

$retum\ \ a$

$return\ Euclid\ GCD\ (b, a \bmod b)$

برای محاسبه $\gcd(412,260)$ از الگوریتم بالا جدول زیر را مشاهده کنید:

| | ۱ | ۲ | ۳ | ٤ | ٥ | ٦ | ۷ |
|---|---|---|---|---|---|---|---|
| **a** | ٤۱۲ | ۲٦۰ | ۱٥۲ | ۱۰۸ | ٤٤ | ۲۰ | ٤ |
| **b** | ۲٦۰ | ۱٥۲ | ۱۰۸ | ٤٤ | ۲۰ | ٤ | ۰ |

بنابراین $\gcd(412,260) = 4$.

## ٦-۲- حساب هم نهشتی

فرض کنید $Z_n$ نمایانگر اعداد صحیح نامنفی کمتر از n باشد $Z_n=\{0,1,2,...,n-1\}$ مجموعه $Z_n$ را مجموعـه باقیمانده‌ها به پیمانه n می‌نامیم .زیرا اگر $b = a \bmod n$ در اینصورت b یک باقیمانده تقسیم a بر n است بنابراین $0 \le b < n$ .

حساب مدولی در $Z_n$ مانند حساب قدیمی است. خواصی مانند تعویض پذیری، جابجایی، جمع و ضرب و داشتن عنصرخنثی برای جمع وضرب. هر عنصر در $Z_n$ دارای یک معکوس جمعی است یعنی برای هر $x \in z_n$ عنصری مانند $y \in z_n$ وجود دارد بطوریکه: $(x+y) \bmod n = 0$

معکوس ضربی $x \in z_n$ را با $x^{-1}$ نمایش می دهیم در اینصورت:

$$x.x^{-1} \equiv 1 \ \ (mod n)$$