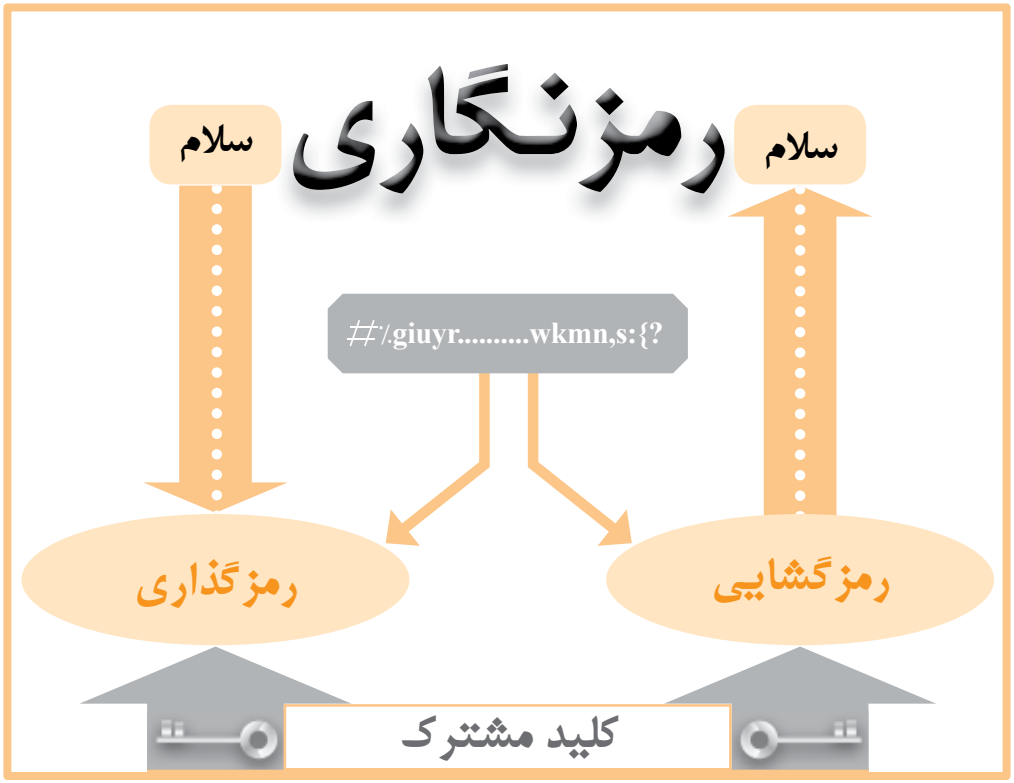
لطافت امیری
دانشجوی دکتری ریاضی محض دانشگاه تربیت‌مدرس



اشاره

یکی از زیباترین و جذاب‌ترین کاربردهای نظریهٔ اعداد «رمزنگاری»[1] اســـت. در ادامه به معرفی یکی از روش‌های ســـادهٔ رمزنگاری می‌پردازیم که از تعریف‌های ابتدایی هم‌نهشتی استفاده می‌کند. ابتدا تعریف هم‌نهشتی را ارائه می‌دهیم.

✱ **تعریف**: برای هر عدد طبیعی مانند m و هر دو عدد صحیح مانـــد a و b، اگر $(a-b)$ بر m بخش‌پذیر باشـــد، a هم‌نهشـــت با b اســـت به پیمانهٔ m و می‌نویسیم: $a \overset{m}{\equiv} b$

مثال.

$۵ \overset{۱۲}{\equiv} -۷$ ، زیرا: $(۵-(-۷)) = ۱۲-$ و $۱۲-$ بر ۱۲ بخش‌پذیر است.

$۲ \overset{۳}{\equiv} ۱۴$، زیـــرا: $(۲-۱۴) = ۱۲$ و ۱۲ بـــر ۳ بخش‌پذیر است.

$۹ \overset{۱۱}{\equiv} ۹$، زیرا: $۹-۹=۰$ و ۰ بر هر عددی بخش‌پذیر است.

تعریف اصطلاحات اولیهٔ رمزنگاری

✱ **متن ساده**[2]: پیامی را می‌گویند که می‌خواهیم به رمز بنویسیم و آن را با P نشان می‌دهیم.

✱ **سیســـتم رمزنویسی**[3]: روشـــی که برای تبدیل متن ســـاده به متن رمزی به‌کار می‌رود، روش‌های متفاوت و زیادی برای رمزنویســـی وجود دارند که بعضی بســـیار پیچیده و غیرقابل گشودن هستند (مثلاً روش بلوکی، کوله‌پشتی و ...).

✱ **متن رمزی**[4]: متنی را که با اســـتفاده از سیســـتم رمزنویســـی به رمز نوشته شـــده است، با C نشان می‌دهیم.

✱ **عملیات رمزگذاری**[5]: عملیات تبدیل متن ســـاده به متن رمزی.

✱ **عملیات رمزگشایی**[۶]: تبدیل متن رمزی به متن ساده یا به عبارت دیگر، گشودن رمز.

✱ **کلید رمز**[۷]: تبدیل مشخصی را از بین تبدیلات ممکن معین می‌کند. این کلید رمز فقط در اختیار نگارندهٔ رمز و دریافت‌کنندهٔ رمز است و آن را معمولاً با k نشان می‌دهیم.

روشی که در اینجا به شما معرفی خواهد شد، به روش «کاراکتر»[۸] معروف است.

در این روش هر حرف از متن ساده به یک حرف دیگر الفبا تبدیل می‌شود و به این ترتیب متن رمزی ساخته می‌شود. به این منظور، ابتدا حرف‌های الفبای انگلیسی را با عددهای ۰ تا ۲۵ نظیر می‌کنیم.

A	B	C	D	E
۰	۱	۲	۳	۴
F	G	H	I	J
۵	۶	۷	۸	۹
K	L	M	N	O
۱۰	۱۱	۱۲	۱۳	۱۴
P	Q	R	S	T
۱۵	۱۶	۱۷	۱۸	۱۹
U	V	W	X	Y
۲۰	۲۱	۲۲	۲۳	۲۴
Z				
۲۵				

در حالت کلی، این جانشینی به ! (۲۶) روش قابل انجام است.

ساده‌ترین نوع روش کاراکتر روش «تبدیل انتقالی»[۹] نام دارد.

در این روش، هر حرف را با k امین حرف بعد از آن جایگزین می‌کنیم. به این صورت که عدد متناظر با هر حرف را با k جمع، و باقی‌ماندهٔ آن را به پیمانهٔ ۲۶ حساب می‌کنیم. باقی‌ماندهٔ به‌دست‌آمده، عدد جدید موردنظر ماست که حرف جدیدی متناظر با آن به ما می‌دهد.

در واقع اگر α را عدد متناظر با حرف اولیه در نظر بگیریم، آن‌گاه β در رابطهٔ پایین عدد جدید مورد نیاز ماست: $\alpha + K \overset{۲۶}{\equiv} \beta$

در اینجا k در واقع همان کلید رمز است که اندازهٔ انتقال هر حرف را مشخص می‌کند و از این نوع ۲۶ تبدیل متفاوت امکان‌پذیر است.

مثال زیر معروف‌ترین مثال از این نوع است.

مثال.

روش **ژولیوس سزار**: این روش توسط سزار به‌کار گرفته می‌شد که در آن k=۳ است. پس: $\alpha + ۳ \overset{۲۶}{\equiv} \beta$

مراحل زیر را انجام می‌دهیم:

عملیات رمزگذاری

i) ابتدا متن سادهٔ P را به بلوک‌های ۵ تایی تقسیم می‌کنیم. دلیل این تقسیم‌بندی آن است که تعداد حرف‌های هر کلمه نیز مشخص نباشد و این تقسیم‌بندی می‌تواند ۴ تایی، ۶تایی یا ... نیز باشد.

C: THIS MESSAGE IS TOP SECRET

P': THISM ESSAG EISTO PSECR ET

ii) با توجه به جدول رمزنگاری، هر حرف متن P را به عدد تبدیل می‌کنیم:

* ۱۹،۷،۸،۱۸،۱۲..... ،۴،۱۹

iii) تبدیل مورد نظر $\alpha + ۳ \overset{۲۶}{\equiv} \beta$ را به‌کار می‌گیریم. یعنی به عددهای بالا سه تا می‌افزاییم و سپس حاصل را به پیمانهٔ ۲۶ حساب می‌کنیم. در این مثال، چون تمام عددها از ۲۶ کمتر هستند، به پیمانهٔ ۲۶ با خودشان برابرند.

** ۲۲،۱۰،۱۱،۲۱،۱۵،..... ،۷،۲۲

IV) حال عددها را به کمک جدول زیر دوباره به حرف تبدیل می‌کنیم:

C:WKLVP HVVDJ HLVWR SVHFU HW

اینجا عمل رمزگذاری پایان می‌پذیرد و متن رمزی را آماده است. حال برای تبدیل متن C به متن P باید عمل رمزگشایی انجام شود.

عملیات رمزگشایی

i) حرف‌های متن C با کمک جدول به عدد تبدیل می‌شوند و عددهای ** را خواهیم داشت.

ii) در این رابطه، هر عدد را باید منهای سه کنیم و سپس به پیمانهٔ ۲۶ حساب کنیم تا به عددهای* برسیم. یعنی باید تبدیل $\beta - ۳ \overset{۲۶}{\equiv} \alpha$ را به‌کار بگیریم.

iii) و در نهایت عددها را به کمک جدول رمز به حرف تبدیل می‌کنیم.

برای مثال، برای چهار حرف WKLV از ابتدای متن C مراحل سه‌گانهٔ بالا را انجام می‌دهیم:

i) طبق جدول رمز داریم:

W	K	L	V
۲۲	۱۰	۱۱	۲۱

مشاهده می‌کنید که این ۴ عدد دقیقاً ۴ عدد ابتدای عددهای ** هستند.

ii) از تبدیل $\beta - ۳ \overset{۲۶}{\equiv} \alpha$ استفاده می‌کنیم و به ترتیب β را ۲۱، ۱۱، ۱۰ و ۲۲ قرار می‌دهیم تا به αهای متناظر برسیم:

$۲۲ - ۲ \overset{۶۴}{\equiv} ۱۹$ $\quad$ $۱۰ - ۳ \overset{۶۴}{\equiv} ۷$

$۱۱ - ۳ \overset{۶۴}{\equiv} ۸$ $\quad$ $۲۱ - ۳ \overset{۶۴}{\equiv} ۱۸$

به ترتیب به عددهای ۱۸، ۸، ۷و ۱۹ می‌رسیم که چهار عدد ابتدای عددهای * هستند.

iii) اکنون به کمک جدول رمز، حرف‌های متناظر با این عددها را پیدا می‌کنیم:

۱۹	۷	۸	۱۸
T	H	I	S

مشاهده می‌کنید که به چهار حرف ابتدای متن P، یعنی THIS رسیدیم.

تمرین ۱

کلمهٔ BORHAN را با کد رمز K =۶ رمزنگاری کردیم و به این حرف‌ها رسیدیم: HUXNG . T حال عملیات رمزگشایی را انجام می‌دهیم:

i) حرف‌ها را به کمک جدول رمز به عددهای متناظر آن‌ها تبدیل می‌کنیم:

H	U	X	N	G
۷	۲۰	۲۳	۱۳	۶

T
۱۹

ii) از تبدیل $\beta - ۶ \overset{۲۶}{\equiv} \alpha$ استفاده می‌کنیم:

$۷ - ۶ \overset{۲۶}{\equiv} ۱$ $\quad$ $۲۰ - ۶ \overset{۲۶}{\equiv} ۱۴$

$۲۳ - ۶ \overset{۲۶}{\equiv} ۱۷$ $\quad$ $۱۳ - ۶ \overset{۲۶}{\equiv} ۷$ $\quad$ $۶ - ۶ \overset{۲۶}{\equiv} ۰$ $\quad$ $۱۹ - ۶ \overset{۲۶}{\equiv} ۱۳$

iii) عددهای ۱۳، ۰،۷، ۱۷، ۱۴، ۱ را که در بالا به‌دست آوردیم، به کمک جدول رمز به حرف‌ها تبدیل می‌کنیم:

۱	۱۴	۱۷	۷	۰	۱۳
B	O	R	H	A	N

تمرین ۲

متن زیرا را با استفاده از جدول رمز و کلید رمز k=۵ رمزگشایی کنید و متن رمزگشایی شده را برای ما بفرستید:

NQTAJ RFYMJ RFYNH

پی‌نوشت‌ها

1.Cryptology
2. Ploin text
3. Cipher
4. Cipher text
5. Enciphering
6. Deciphening
7. Key
8. Character
9. Shilt transformation