



اشاره

در قسمت قبل با مقدمه‌ای از رمزنگاری‌های متعارف در قرون گذشته به صورت توصیفی آشنا شدید. در این قسمت و قسمت‌های بعدی با اصول رمزنگاری و رمزگشایی‌های «تک‌الفبایی حاصل از الفبای متعارف مستقیم»، «رمزهای تک‌الفبایی مبتنی بر تبدیل‌های خطی» و «سیستم‌های چندحرفی» و... آشنا خواهید شد. در این قسمت به رمزهای تک‌الفبایی حاصل از الفبای متعارف مستقیم (رمز جای گذاری) می‌پردازیم. در آخر نیز برای آزمودن یافته‌ها، چند تمرین خواهیم آورد.

هم‌نهشتی و کاربردهای آن رمزنگاری و رمزگشایی (۱۲)

سید محمدرضا هاشمی موسوی
hashemi_moosavi@yahoo.com

کلیدواژه‌ها: پیام رمز، رمز جای گذاری، دنباله‌ی صریح، دنباله‌ی رمزی، رمزهای تک‌الفبایی، الفبای جای گذاری، عدد کلیدی، کلید رمز، فراوانی حروف.

رمزهای تک‌الفبایی حاصل از الفبای متعارف مستقیم
(رمز جای گذاری)

رمز سزاری

یکی از قدیمی‌ترین سیستم‌های رمزنگاری که می‌شناسیم، سیستمی است که ژول سزار به کار برده و به همین مناسبت به

رمزنگاری سزاری موسوم است. در این روش رمزنگاری به جای هر حرف از پیام، حرف سوم بعد از آن از حروف الفبای معمولی قرار داده می‌شد. البته سزار الفبای رومی را به کار می‌برد، ولی ما شیوه‌ی او را با الفبای امروزی (انگلیسی) شرح خواهیم داد. فرض کنید بخواهیم پیام زیر را به رمز درآوریم:

«I CAME I SAW I CONQUERED»

ابتدا زیر هر حرف از پیام، حرفی را می‌نویسیم که در حرف‌های الفبا به ترتیب معمول، سه حرف پس از آن قرار گرفته است، یعنی به جای I حرف L قرار می‌گیرد، به جای C حرف F، به جای A حرف D، به جای I حرف L، به جای S حرف V، به جای A حرف D، به جای W حرف Z، به جای I حرف L، به جای C حرف F، به جای O حرف Q، به جای N حرف T، به جای Q حرف X، به جای U حرف H، به جای E حرف U، به جای R حرف G.

متن اصلی :	I	C	A	M	E	I	S	A	W	I	C	O	N	Q	U	E	R	E	D
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
پیام رمزی :	L	F	D	P	H	L	V	D	Z	L	F	R	Q	T	X	H	U	H	G

بنابراین، پیام رمزی چنین است:

«L FDPH L VDZ L FRQTXHUHG»

نتیجه کاملاً نامفهوم به نظر می‌رسد. برای فردی که آن را بررسی می‌کند و از چگونگی تهیه‌ی آن اطلاعی ندارد، ممکن است تلاش برای کشف آن کاملاً بی‌ثمر باشد. از طرف دیگر برای کسی که رمز را می‌داند، معنای پیام به سرعت معلوم می‌شود. فقط کافی است به جای هر حرف از پیام رمزی، حرفی را که در حرف‌های الفبا به ترتیب معمولی سه حرف پیش از آن قرار گرفته است جایگزین کنیم تا مطلب اصلی فاش شود.

این مثالی از نوعی رمز به نام «رمز جای‌گذاری» است که در آن به جای هر حرف از پیام اصلی حرف دیگری گذاشته می‌شود. راهی مناسب برای نمایش دادن به این جای‌گذاری استفاده از «الفبای جای‌گذاری» است که نشان می‌دهد چه حرفی به جای چه حرف دیگر قرار می‌گیرد. روش ساختن الفبای جای‌گذاری در رمز سزاری، عبارت از نوشتن دنباله‌ی الفبای معمولی در یک سطر و سپس بازنویسی آن در سطر دوم، منتها با شروع از D به جای A است. وقتی که در سطر دوم به حرف آخر الفبا رسیدیم، بعد از حرف Z به ترتیب حرف‌های A، B و C را می‌نویسیم، درواقع دنباله‌ی الفبا را به صورت چرخه‌ای در نظر می‌گیریم که به‌طور متوالی تکرار می‌شود:

دنباله‌ی صریح ۱):	A	B	C	D	E	F	G	H	I	J	K	L	M	N	R	...	X	Y	Z
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
دنباله‌ی رمزی ۲):	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	...	A	B	C

سطر اول را دنباله‌ی صریح و سطر دوم را دنباله‌ی رمزی می‌خوانیم. به این ترتیب، عمل به رمز درآوردن را می‌توانیم به این صورت انجام دهیم که به جای هر حرف از پیام صریح، حرف زیرین آن در الفبای جای‌گذاری را قرار دهیم. برای رمزگشایی می‌توانیم به جای هر حرف از پیام رمزی، حرف بالایی آن در الفبای جای‌گذاری را بگذاریم (به بیان ریاضی می‌گوییم عمل از رمز درآوردن معکوس عمل به رمز درآوردن است). فرایند رمزنگاری در رمز سزاری را می‌توان به صورت عددی نیز انجام داد. فرض کنید به هر حرف، عددی اختصاص دهیم که مکان آن را در دنباله‌ی معمولی الفبا (شکل صریح) نشان دهد. در این صورت تناظر زیر را خواهیم داشت:

دنباله‌ی صریح :	A	B	C	D	E	F	G	H	I	J	K	L	M	...	X	Y	Z
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
دنباله‌ی رمزی :	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	...	۲۴	۲۵	۲۶

حال برای به رمز درآوردن پیام مورد نظر، به طریق زیر، مرحله به مرحله، عمل می‌کنیم:

۱) به جای هر حرف، عدد متناظر با آن را قرار می‌دهیم.

(۲) به هریک از این اعداد ۳ واحد اضافه می‌کنیم.
(۳) به جای اعداد حاصل، حروف متناظرشان را می‌گذاریم.

(مرحله ۱): I	C	A	M	E	I	S	A	W	I	C	O	N	Q	U	E	R	E	D
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
۹	۳	۱	۱۳	۵	۹	۱۹	۱	۲۳	۹	۳	۱۵	۱۴	۱۷	۲۱	۵	۱۸	۵	۲

(مرحله ۲): ۱۲	۶	۴	۱۶	۸	۱۲	۲۲	۴	۲۶	۱۲	۶	۱۸	۱۷	۲۰	۲۴	۸	۲۱	۸	۷
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
(مرحله ۳): L	F	D	P	H	L	V	D	Z	L	F	R	Q	T	X	H	U	H	G

همان‌طور که انتظار داشتیم، نتیجه همان پیام رمزی است که از پیش به‌دست آمده بود.
تمرین. پیام زیر را که با رمز سزاری به رمز درآمده است، از رمز درآورید.

۱. FRZDUGV GLH PDQB WLP HV EHIRUH WKHLU GHDWKV

الفبای متعارف مستقیم

نمی‌دانیم چرا سزار عدد ۳ را به‌عنوان میزان انتقال دنباله‌ی رمزی نسبت به دنباله‌ی صریح انتخاب کرد. او می‌توانست هر عددی را برای این منظور به‌کار ببرد، فقط کافی بود که از پیش با طرف مکاتبه‌ی خود درباره‌ی چگونگی به رمز درآوردن، قراری گذاشته باشد. درواقع، به فرض یک قرارداد مناسب، میزان انتقال می‌تواند در هر پیام با پیام دیگر فرق داشته باشد. برای مثال، می‌توان قرار گذاشت که طبق طرحی، به هر پیام یک عدد نسبت داده شود و باقی‌مانده‌ی این عدد به یک عدد ثابت مانند ۲۶ (تعداد حروف الفبای لاتین)، میزان انتقال یعنی مقدار تغییر مکان گرفته شود. برای مثال، چنین عددی ممکن است به یکی از این ویژگی‌ها مختص شود: به تعداد کلمات هر پیام، شماره‌ی پیام و تاریخ ماهی که پیام فرستاده می‌شود، عددی که از یک فرایند به‌دست می‌آید که اصلاً ربطی به آن مکاتبه ندارد.

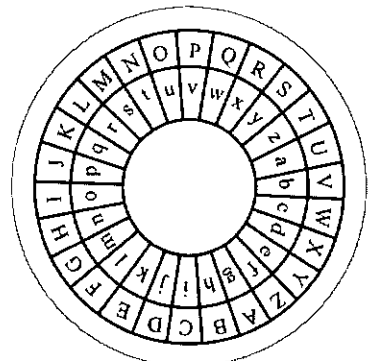
در هر صورت با داشتن این عدد، الفبای جایگزین می‌تواند ساخته شود و هم در به رمز درآوردن و هم در از رمز درآوردن به کار رود. یک الفبای جای‌گذاری که در آن هم دنباله‌ی صریح و هم دنباله‌ی رمزی از الفبای معمولی گرفته شده باشد (به این ترتیب که دنباله‌ی رمزی پس از مقدار مشخصی تغییر مکان به دست آمده باشد). «الفبای متعارف مستقیم» خوانده می‌شود.

در فرایند عددی معادل می‌توان گفت: $C=P+K$ ؛ که در آن K ، مقدار تغییر مکان، عددی است که باید به P ، معادل عددی هر حرف زبان صریح، اضافه شود تا C ، جانشین رمزی آن، به‌دست آید. اگر مقدار تغییر مکان K باشد، آن‌گاه حرف A از دنباله‌ی صریح مقابل حرفی از دنباله‌ی رمزی واقع است که متناظر با $(K+1)$ است.

با ابزاری ساده به سرعت می‌توان الفبای متعارف مستقیم را تشکیل داد. این ابزار از دو دایره‌ی هم‌مرکز ساخته می‌شود که در پیرامون هریک از آن‌ها، حرف‌های الفبا به‌ترتیب نوشته شده‌اند (مطابق شکل ۱).

حلقه‌ی بیرونی دنباله‌ی صریح و حلقه‌ی درونی که قابل چرخیدن است، دنباله‌ی رمزی است. اگر مقابل A از حلقه‌ی بیرونی، حرف متناظر $(K+1)$ از حلقه‌ی درونی را قرار دهیم، الفبای جای‌گذاری را که میزان انتقال آن K باشد، خواهیم داشت (شکل ۱) برای حالت $K=6$ رسم شده است). جالب توجه است که سال‌ها پیش، ارتش آمریکا ابزار مشابهی را به‌کار می‌برد. الفبایی که این ابزار تولید می‌کرد، با الفبای متعارف مستقیم این تفاوت را داشت که دنباله‌ی رمزی در آن به‌ترتیب وارونه نوشته شده بود. چنین دنباله‌ای «دنباله‌ی متعارف وارونه» و الفبایی که این دنباله با قرار گرفتن در مقابل دنباله‌ی صریح معمولی تولید می‌کند «الفبای متعارف وارونه» نامیده می‌شود.

اگر از دایره برای ساختن الفبای متعارف مستقیم استفاده کنیم، آن‌گاه انتخاب هریک از ۲۶



شکل ۱

طبق آن میزان انتقال معلوم شود چنین عددی به دست آید، باید در این قرار مشخص شده باشد که چه عددی جانشین آن شود.

هر سیستم رمزنگاری دو اصل اساسی دارد: سیستم کلی و کلید ویژه.

«فرایند کلی مورد استفاده و جزئیات نحوه‌ی استفاده از آن فرایند کلی را سیستم کلی و مشخص‌کننده‌ی جزئیات نحوه‌ی استفاده از این فرایند را کلید ویژه می‌نامند.» برای مثال در رمزنگاری سزاری از یک الفبای متعارف مستقیم با کلید ویژه‌ی ۳ استفاده می‌شود. از آنجا که در این سیستم تنها یک الفبای جای‌گذاری به‌کار می‌رود، نتیجه را «رمز تک‌الفبایی» می‌نامند.

تمرین

۱) یک الفبای متعارف مستقیم با میزان انتقال ۷ بازید و پیام زیر را به رمز درآورد:

THE FAULT DEAR BRUTUS IS NOT IN OUR STARS
BUT IN OURSELVES.

۲) پیام رمزی زیر را با دانستن آن که الفبای متعارف مستقیم آن با میزان انتقال ۱۱ است، از رمز درآورد.

ESPCPTDLETOP TYESPLQQLTCDZQXPYHSTNS
ELVPY LE ESP QWZZO WPLOD ZY EZ QZCEFP.

ياسمها

1) AOL MHBSA KLHY IYBABZ PZ UVA PU VBY
ZAHYZ IBA PU VBYZLSCLZ.

2) THERE IS A TIDE IN THE AFFAIRS OF MEN
WHICH TAKEN AT THE FLOOD LEADS ON THE
FORTUNE.

پی نوشت

3. Vigenère

این چند سطر مربوط به انتهای مقاله‌ی قسمت (۱۱) در مجله‌ی رشد برهان شماره‌ی ۶۸ است که به علل اشکالات چاپی، حذف شده بود:

«فارغ التحصیلان ریاضیات پیشرفته در ارتش‌ها و دستگاه‌های اطلاعاتی؛ کارطراحی سیستم‌های رمزی، و شکستن رمزهای حریف به کارگیری انواع دستگاه‌های رمزنگار رایانه‌ای، و طراحی سیستم‌های کدینگ مشغول‌اند.

امروزه رمزهای دستی و قراردادی، جای خود را به سیستم‌های پیچیده‌ی دیجیتالی و نوآوری‌هایی در زمینه‌های رمزهای مخفیانه و ارتباط داده‌اند.»