اشاره

در قسمت قبل با مقدمه‌ای از رمزنگاری‌های متعارف در قرون گذشته به‌صورت 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 جای‌گذاری) 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 جای‌گذاری، دنباله‌ی صریح، دنباله‌ی رمزی، رمزهای تک‌الفبایی، الفبای جای‌گذاری، عدد کلیدی، کلید رمز، فراوانی حروف.

رمزهای تک‌الفبایی حاصل از الفبای متعارف مستقیم (رمز جای‌گذاری)

رمز سزاری

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

رمزنگاری سـزاری موسـوم 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 به‌کار 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 به‌ترتیب 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 و غیره. نتیجه‌ی کار چنین است:

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 به‌نظر می‌رسـد. برای فردی که آن را بررسـی می‌کند و از چگونگی تهیه‌ی آن اطلاعی ندارد، ممکن اسـت تلاش برای کشـف آن کاملاً بی‌ثمر باشـد. از طرف دیگر برای کسـی که رمز را می‌داند، معنای پیام به سـرعت معلوم می‌شود. فقط کافی است به جای هر حرف از پیام رمزی، حرفی را که در حرف‌های الفبا به‌ترتیب معمولی سـه حرف پیش از آن قرار گرفته اسـت جایگزین کنیم تا مطلب اصلی فاش شود.

این مثالی از نوعی رمز به نام «**رمز جای‌گذاری**» اسـت که در آن به جای هر حرف از پیام اصلی حرف دیگری گذاشـته می‌شـود. راهی مناسـب برای نمایش دادن به این جای‌گذاری اسـتفاده از «**الفبای جای‌گذاری**» است که نشان می‌دهد چه حرفی به جای چه حرف دیگر قرار می‌گیرد. روش سـاختن الفبای جای‌گذاری در رمز سـزاری، عبارت از نوشـتن 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 به‌ترتیب حرف‌های A، B و C را می‌نویسیم، درواقع دنباله‌ی الفبا را به‌صورت 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 اسـت). فرایند رمزنگاری در رمز سـزاری را می‌توان به‌صورت 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	٤	٥	٦	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	....	۲٤	۲٥	۲٦

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.

I : (مرحله‌ی 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	۴
۱۲ : (مرحله‌ی ۲)			۶	۴	۱۶	۸		۱۲		۲۲	۴	۲۶		۱۲		۶	۱۸	۱۷	۲۰	۲۴	۸	۲۱	۸	۷
	↓		↓	↓	↓	↓		↓		↓	↓	↓		↓		↓	↓	↓	↓	↓	↓	↓	↓	↓
L : (مرحله‌ی ۳)			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 WLPHV EHIRUH WKHLU GHDWKV

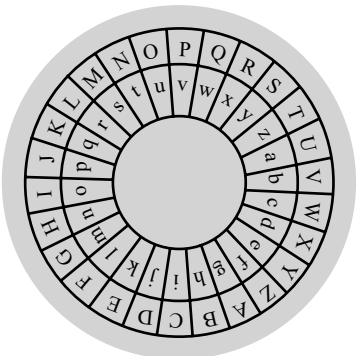
الفبای متعارف مستقیم

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 عددیِ 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+۱) 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).

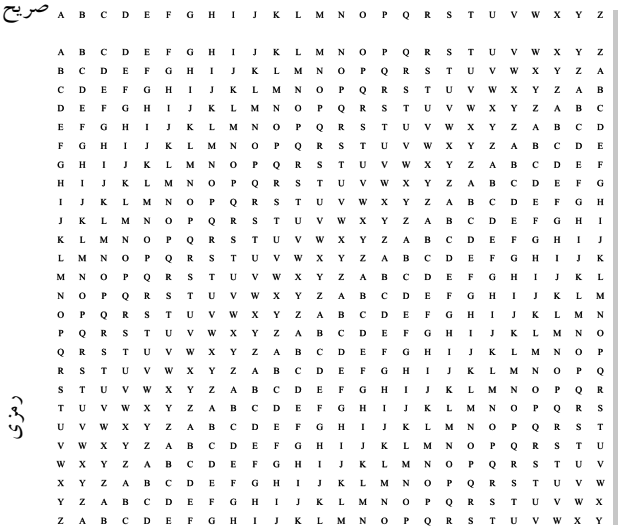


شکل ۱

حلقه‌ی بیرونی دنباله‌ی صریح و حلقه‌ی درونی که قابل چرخیدن است، دنباله‌ی رمزی است. اگر مقابل A از حلقه‌ی بیرونی، حرف متناظر (K+۱) از حلقه‌ی درونی را قرار دهیم، الفبای جای‌گذاری را که میزان انتقال آن K باشد، خواهیم داشت (شکل (۱) برای حالت K=۶ 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

الفبای متعارف مستقیم با قرار دادن دایره‌ی درونی در وضع مناسب امکان‌پذیر می‌شود. چنین امکانی را «ویژنر»[1] رمزنگار فرانسوی به طریقی دیگر فراهم آورد. او در یک مربع حرف‌های الفبا را نوشت، به این طریق که در بالاترین سطر، دنباله‌ی معمولی الفبا را نوشت و در هر سطر متعاقب آن، دنباله‌ای را نوشت که از انتقال دنباله‌ی قبلی به اندازه‌ی یک حرف به سمت چپ به دست می‌آمد. با قرار دادن الفبای معمولی به‌عنوان دنباله‌ی صریح در بالای مربع، هر الفبای متعارف مستقیم از ترکیب دنباله‌ی صریح با یک سطر مناسب در مربع، قابل حصول بود. هریک از این الفباها به‌راحتی با اولین حرف دنباله‌ی رمزی آن معین می‌شد (شکل ۲).



توجه: این مربع اساس سیستم‌هایی است که هریک از آن‌ها را بیان خواهیم کرد.

درباره‌ی قراری که برای تعیین میزان انتقال گذاشته می‌شود، نکته‌ای را باید متذکر شویم. واضح است که اگر طبق قرار ما عدد تعیین‌کننده‌ی کلید رمز پیام بتواند مضربی از ۲۶ باشد، مرتکب اشتباه شده‌ایم، زیرا چنین عددی در تقسیم بر ۲۶ باقی‌مانده‌ای برابر صفر خواهد داشت و درنتیجه پیام باید به زبان معمولی نوشته شود. بنابراین، قرار ما باید به گونه‌ای باشد که طبق آن نتوان عدد ۲۶ (یا هر مضربی از آن) را به‌عنوان میزان انتقال به‌کار برد؛ اگر از فرایندی که قرار است طبق آن میزان انتقال معلوم شود چنین عددی به‌دست 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 بسازید و پیام زیر را به رمز درآورید:

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 درآورید.

ESPCP TD L ETOP TY ESP LQQLTCD ZQ XPY HSTNS ELVPY LE ESP QWZZO WPLOD ZY EZ QZCEFYP.

پاسخ‌ها

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

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

پی‌نوشت

۱. Vigenére

پوزش و اصلاح

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

«فارغ‌التحصیلان ریاضیات پیشرفته در ارتش‌ها و دستگاه‌های اطلاعاتی؛ کارطراحی سیستم‌های رمزی، و شکستن رمزهای حریف به‌کارگیری انواع دستگاه‌های رمزنگار رایانه‌ای، و طراحی سیستم‌های کدنیگ مشغول‌اند.

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