

دو فصلنامه علمی تاریخ‌نگاری و تاریخ‌نگاری دانشگاه الزهرا (س)
سال بیست و نهم، دوره جدید، شماره ۲۴، پیاپی ۱۰۹، پاییز و زمستان ۱۳۹۸ / صفحات ۱۸۷-۱۶۵
مقاله علمی - پژوهشی

رمزنگاری در دوره قاجار؛ گذر از رمزنگاری سنتی به رمزنگاری نوین^۱

صمد کاوسی رکعتی^۲

تاریخ دریافت: ۹۸/۰۸/۱۳

تاریخ پذیرش: ۹۹/۰۳/۰۸

چکیده

از زمان‌های دور برای ارسال پیغام‌های محرمانه بین جوامع بشری، ارتباطات رمزی وجود داشته است. در تاریخ ایران نیز رمزنویسان از اقلام رمزی زیادی استفاده می‌کردند. بعد از پدید آمدن تلگراف، اقلام رمزی قدیمی کنار گذاشته و اقلام جدیدی اختراع شد و در مکاتبات و گزارش‌های محرمانه به کار رفت. در این پژوهش با بهره‌گیری از منابع کتابخانه‌ای و به‌خصوص کتاب‌های چاپ سنگی و نیز اسناد تاریخی سعی شد به سؤال محوری چرایی از بین رفتن اقلام و خطوط سابق و چگونگی اختراع اقلام جدید رمزنگاران ایرانی و نیز تلاش آنان برای یافتن راه‌حلی به منظور رفع مشکلات ارتباطات رمزی از طریق کانالی امن در دوره قاجار، پاسخ داده شود. نتیجه این پژوهش نشان می‌دهد که در دوره قاجار به دلیل آغاز ارتباطات سیاسی و اقتصادی گسترده با دنیای غرب، آشنایی با رمزنگاری مدرن غربی‌ها و نیز پی‌بردن به سادگی و مشکلات استفاده از رمزنویسی سنتی، نیاز به استفاده از رمزنگاری پیشرفته در ارتباطات رمزی و به‌خصوص در تلگراف‌ها احساس شد. بنابراین عده‌ای از رمزشناسان ایرانی در این راستا اقلام رمزی جدیدی پدید آوردند که برای ارسال پیغام‌های رمزی داخلی و خارجی از اطمینان لازم برخوردار بود.

واژگان کلیدی: رمز، رمزنگاری، رمزنگاری نوین، دوره قاجاریه، اسناد تاریخی

۱. شناسه دیجیتال (DOI): 10.22051/HPH.2020.32381.1456

۲. کارشناس ارشد تاریخ ایران اسلامی، کارشناس اسناد تاریخی سازمان اسناد و کتابخانه ملی ایران:
kavousiarad98@yahoo.com

مقدمه

رمز کلمه‌ای عربی است از مصدر مجرد، باب فَعَلَ يَفْعُلُ که در زبان فارسی بسیار کاربرد دارد. رمز یعنی به لب، چشم، ابرو یا به دهان و زبان اشاره کردن. این واژه به معانی دیگری نیز به کار رفته است: اشاره، رمز، سر، ایما، دقیقه، نکته، معما، نشانه، اشاره پنهان، نشانه مخصوصی که از آن مطلبی درک شود، چیز نهفته میان دو یا چند کس که دیگری بر آن آگاه نباشد و مقصود با نشانه‌ها و علائم قراردادی و معهود بیان شود. آنچه در تمام این معانی مشترک است صریح نبودن و پوشیدگی است. (مفتاح‌الملک، ۱۳۱۳ق: ۱۱۵؛ شیخ‌زادگان، ۱۳۸۹: ۶؛ محمدی فشارکی و دیگران، ۱۳۹۰: ۱۱۸) رمزنگاری، معادل واژه کریپتوگرافی انگلیسی است و از واژه کریپتوس مشتق شده است و موضوع آن پرداختن به مباحث و مسائل مرتبط با تبدیل پیغامی آشکار (اصلی) به پیغامی رمزی با استفاده از روش و الگوی مشخص (الگوریتم) و یک یا چند کلید است. (شیخ‌زادگان، ۱۳۸۹: ۶) رمزنگاری نزد مسلمانان به تعمیمه یا معماسازی مشهور بوده و از روش‌های مختلفی برای ارسال پیغام رمز استفاده می‌کردند. درخصوص موضوع بحث شده در این پژوهش تحقیق مستقلی صورت نگرفته است، اما درباره رمزنگاری در متون قدیمی به‌خصوص پیش از قاجار نویسندگان، نه از منظر تاریخی، بلکه ادبی و نیز کاربرد رمز در علوم غریبه به این موضوع پرداخته اند و کتاب‌ها و مقالات و مدخل‌هایی نیز به نگارش درآمده است، از جمله:

کتاب *اسرار و رموز اعداد و حروف* نوشته احمد آقاشریف که در این کتاب به تاریخچه و شرح رابطه حروف و اعداد و تقدس آنها پرداخته است. کله سر تألیف ارسلان کشوری که مخفف پنج کلمه کیمیا، لیمیا، هیمیا، سیمیا و ریمیا است و در این کتاب به شرح علوم سیری پرداخته شده و نیز تقدس حروف و اعداد و چگونگی رمزنویسی با حروف را شرح داده است. رمزنویسی و گویش‌های رمزی، نوشته نرگس محمودی که در آن به تاریخچه‌ای از رمزنگاری در دنیا و نیز مختصری از شیوه‌های رمزنگاری و رمزگشایی و نیز زبان‌های رمزی اشاره شده است. حروف رمزی در فرهنگ و تمدن ایران تألیف عیسی صفری ممقانی که به کلیاتی از تاریخ رمزنگاری و شیوه‌های آن تا دوره معاصر پرداخته شده است. مقاله‌های «ابداع خطوط رمزی در فرهنگ اسلامی و ایرانی» از مصطفی ذاکری، «رمزنگاری در نامه‌ها (برگرفته از صبح الأعشی فی صناعة الإنشاء فلقشندی)» از هادی عالم‌زاده که در واقع شرحی از شیوه‌های رمزنگاری مسلمانان از زبان ابن‌دریهم رمزنگار معروف است، «خط شجری» از سید علی کسایی که در این مقاله شیوه رمزنویسی با خط شجری آمده است، خط معما (پژوهش در انواع و شیوه‌های رمزنگاری منشآت) از محسن محمدی فشارکی و مریم شیرانی که

نویسندگان مقاله به استفاده از خطوط رمز و انواع آن در متون تاریخی و مکاتبات محرمانه و نیز پنهان‌نویسی در دوران اسلامی پرداخته‌اند. این پژوهش با هدف بررسی تلاش رمزشناسان ایرانی در دوره قاجار به منظور پدیدآوردن اقلام رمزی جدید در ارتباطات رمزی و محرمانه، سعی دارد به چرایی نادیده‌گرفتن اقلام رمزی سنتی و چگونگی اختراع اقلام جدید این رمزشناسان پاسخ دهد.

رمزنگاری سنتی و پیشینه آن

تعیین تاریخ دقیقی برای مبدأ ارتباطات رمزی در تاریخ بشر دشوار به نظر می‌رسد. بشر تا پیش از اختراع خط برای انتقال منظور و پیام خود از اشکال، علائم و نشانه‌های خاص سود می‌جست. شاید بتوان این اشکال، علائم و نشانه‌ها را مبنای شکل‌گیری رمزنگاری تصور کرد، به‌خصوص اگر بین چند نفر یا گروه خاصی رد و بدل شده باشند. رمزنگاری در نقاط مختلف دنیا به اشکال گوناگون وجود داشته است. مثلاً اقوام اینکا (مردمی دارای تمدن نسبتاً پیشرفته در پرو) به منظور برقراری ارتباط با یکدیگر از ریسمان‌های رنگی استفاده می‌کردند که به شیوه‌های گوناگون آنها را گره می‌زدند، تعداد گره‌های موجود در این ریسمان‌ها دارای معانی خاصی بود. این ریسمان‌ها که در زبان بومی پرو «کوئیپو» نام داشت، افراد خاصی آن را گره می‌زدند که برای این منظور تعلیم دیده بودند و فقط همین افراد بودند که می‌توانستند معنی آن را آشکار کنند. (صفری ممقانی، ۱۳۹۶: ۵۶) از لحاظ تاریخی در هیروگلیف‌های مصری، آثاری از رمز به معنای اخص آن پیدا شده است و همچنین پس از اختراع خط و در میان هندی‌ها، بابلی‌ها، آشوری‌ها، اسپارتی‌ها و امپراطوران چین باستان هم نمونه‌های تاریخی از رمزنگاری موجود است. اعداد و حروف تقریباً نزد بیشتر اقوام باستانی دارای منزلت خاصی بوده و علاوه بر استفاده از اعداد و حروف در رمزنویسی، با کمک‌گرفتن از ارتباطات اعداد و حروف، به تأویل و تعبیر حوادث و رؤیا و تفسیر جهان می‌پرداختند. دانستن علم حروف و اعداد از ضروریات علوم غریبه بوده است. (کشوری، ۱۳۸۴: ۲۳۴-۲۳۳)

در چین از خط اندیشه‌نگار که ترکیبی از واژه‌ها و نمادها بود، برای رمزنویسی کمک می‌گرفتند (محمدی فشارکی، شیرانی: ۱۱۱) خط نسبییدی (Nsibidi) متعلق به اوگام نیجریه نیز خطی اندیشه‌نگار است که در آن از نشانه‌های تصویری کاملاً قراردادی و اشکال نمادین استفاده می‌شده است. (اسماعیل‌پور، ۱۳۸۹: ۱۸۵-۱۸۴) در روم باستان از خط هیروگلیف مصری برای رمزنگاری استفاده می‌شد و برخی از نشانه‌ها را با نشانه‌هایی که به آنها شبیه بود، تعویض می‌کردند و واژه‌های پیچیده به وجود می‌آوردند که جز برای افراد آشنا به کلید رمز،

فهمیدنی نبود. (محمدی فشارکی، شیرانی، ۱۳۹۰: ۱۱۱) گذشته از این رمزنگاری جولیس سزار رمز دیگری بود که رومیان استفاده می کردند. این رمزنگاری ساده ترین رمز جانشینی بود که در آن تمامی حروف به میزان یک گام مشخص جابه جا می شدند. (شیری، ۱۳۹۳: ۱۷)

در خصوص رمزنگاری در ایران پیش از ساسانیان اطلاعات چندانی در دست نیست. در *المهرست* ابن ندیم و به نقل از ابن مقفع، ایرانیان پیش از اسلام دارای هفت نوع خط بوده اند، از جمله این خطوط که هر کدام را جداگانه شرح می دهد، می توان به دین دبییره، ویش دبییره، کشتج، نیم کشتج، شاه دبییره (خط مخصوص مکاتبات شاهان) وهام دبییره (خط ویژه تمام طبقات مملکت)، رازسهریه (جهت نگارش اسرار پادشاهان برای اشخاص سایر ملل) و راس سهریه اشاره کرد. در این بین خط ویش دبییره خطی رمزی محسوب می شده است. (ابن ندیم، ۱۳۸۱: ۲۲)

عده ای نیز پدید آمدن علم حروف و جفر را به ایرانیان نسبت می دهند و معتقدند که علم مغانه یکی از علوم بوده که تعداد محدودی از مغان، آن را می آموختند و به عده محدود دیگری تعلیم می دادند. (ملکان سرشت، ۱۳۸۱: ۳) بشر گذشته از استفاده از رمز در مکتوبات، در ارتباطات کلامی نیز از رمز بهره می جست. از این زبان های رمزی می توان به زبان زرگری، زبان لاتی، زبان مخفی یا زبان آرگو (Argo) اشاره کرد. سارقان، زندانیان، متکدیان، بدنامان و معتادان به استفاده از این زبان های رمزی پرداختند. (محمدی فشارکی و دیگران، ۱۳۹۰: ۱۱۰)

در تعریف دقیق زبان رمزی می توان گفت زبانی است ساختگی که دو یا چند تن، یا گروهی از مردم در میان خود قرارداد می کنند تا هنگامی که بخواهند معنا و راز سخنانشان برای دیگران پوشیده و پنهان بماند، با آن گفت و گو کنند. اساس ساختن آن، همان زبانی است که مردم یک آبادی یا یک شهر با آن صحبت می کنند، ولی کلمات را طوری دستکاری می کنند که غیر از افراد آن گروه، کسی آن را نمی فهمد. این نوع زبان بین اصناف و پیشه وران و برخی اقلیت های ایران مانند یهودیان یا گروه های کوچکی مثل کولی ها رواج دارد. (محمودی، ۱۳۸۹: ۴۲)

مسلمانان و رمزنگاری

با توجه به شروع بعضی از سوره های قرآن با حروف مقطعه و رمزگونه بودن این حروف، از همان ابتدا مسلمانان به اهمیت رمزنگاری پی بردند و کنجکاوی و تلاش های زیادی برای حل این حروف رمزی انجام دادند. اما به طور جدی رمزنگاری از قرن دوم هجری توجه دانشمندان و کاتبان جهان اسلام را به خود جلب کرد تا جایی که به عنوان یک علم مستقل درباره آن کتاب نوشتند. اولین کتاب ها درباره رمزنگاری و علم تعمیه را خلیل بن احمد فراهیدی و جابر بن حیان

تاریخ‌نگاری و تاریخ‌نگاری، سال ۲۹، شماره ۲۴، پاییز و زمستان ۱۳۹۸ / ۱۶۹

تألیف کردند؛ اما این کتاب‌ها از بین رفته و به دست ما نرسیده است. قدیمی‌ترین مکتوب به جا مانده از این علم، رساله فی استخراج المعمی اثر الکندی (متوفی ۲۶۰ ق) است. (محمدی فشارکی و دیگران، ۱۳۹۰: ۱۱۲) بعد از این کتاب، مسلمانان کتاب‌های بسیاری را در خصوص رمز و و روش‌های رمزنگاری نوشتند.

مسلمانان در رمزنویسی که به آن تعمیمه یا معماسازی می‌گفتند، از روش‌های مختلفی بهره می‌بردند که از آن جمله می‌توان به این روش‌ها اشاره کرد:

۱. جابه‌جایی محل حروف در کلمات: در این روش حروف هر کلمه برعکس می‌شود؛ یعنی از آخر به اول نوشته می‌شود یا حروف کلمه را دوتا دوتا جایگزین هم می‌کردند مثلاً به جای نوشتن محمد، «حمدم» می‌نوشتند؛

۲. عوض کردن جای حروف الفبا: در این روش هر حرف در جایگاه حرف بعد از خود قرار می‌گیرد؛ یعنی الف به جای ب، ب به جای ت و... ی به جای الف.

۳. افزودن یا کاستن حرفی از حروف کلمات. (همان: ۱۱۴-۱۱۳؛ عالم‌زاده، ۱۳۹۰: ۶۴-)

(۶۳)

یکی از روش‌های رمزنویسی مسلمانان، استفاده از حروف ابجد بود که خود یکی از دوایر حروف در زبان عربی به شمار می‌رود. ترتیب حروف را به اصطلاح دوایر حروف می‌گویند، مثلاً دایره ابث یا ابثی، مقصود ترتیب حروف است به شکل ا ب ت ث ج ح و... که از معروف‌ترین دوایر حروف به‌شمار می‌رود. هم‌چنین دایره ابجد یا ابجدی یعنی ترتیب حروف به جمل: ابجد، هوز، حطی، کلمن، سعفص، قرشت، ثخذ و ضطع که این دایره هم معروف و در نوشتن حروف تقویم و گفتن ماده تاریخ معمول است. اما دوایر مشهور و معمول که علمای فن ترتیب و مبنای عمل قرار داده‌اند، سیزده دایره است: ابث، ابجد، اهطم، اجهب، ایقغ، اجذش، ارغی، انسغ، احست، ادیل، اجهب، افسج و اعطط. (کشوری، ۱۳۸۴: ۴۱) در کتاب بلایع العلوم کنزالرموز فی علم الفنون، تعداد دوایر بیست و هشت مورد ذکر شده است. (فانی تبریزی، ۱۳۰۰ ق: ۱۰-۶)؛ اما حروف ابجد خود به سه قسمت ابجد صغیر، وسیط و کبیر تقسیم شده است. (کشوری، ۱۳۸۴: ۳۴)

۱۷۰ / رمزنگاری در دوره قاجار؛ گذر از رمزنگاری ستی به رمزنگاری نوین / صمد کاوسی رکعتی

ابجد صغیر

۱	ب	ج	د	ه	و	ز	ح	ط	ی
۱	۲	۳	۴	۵	۶	ساقط	۱	۲	۳
ک	ل	م	ن	س	ع	ف	ص	ق	ر
۴	۲	۵	۱	۴	ساقط	۳	۶	۲	۴
ش	ت	ث	خ	ذ	ض	ظ	غ		
۶	۱	۳	۵	ساقط	۲	۴	۶		

ابجد وسیط

۱	ب	ج	د	ه	و	ز	ح	ط	ی
۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
ک	ل	م	ن	س	ع	ف	ص	ق	ر
۸	۶	۴	۲	ساقط	۱۰	۸	۶	۴	۸
ش	ت	ث	خ	ذ	ض	ظ	غ		
ساقط	۴	۸	ساقط	۴	۸	ساقط	۴		

ابجد کبیر

۱	ب	ج	د	ه	و	ز	ح	ط	ی
۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
ک	ل	م	ن	س	ع	ف	ص	ق	ر
۲۰	۳۰	۴۰	۵۰	۶۰	۷۰	۸۰	۹۰	۱۰۰	۲۰۰
ش	ت	ث	خ	ذ	ض	ظ	غ		
۳۰۰	۴۰۰	۵۰۰	۶۰۰	۷۰۰	۸۰۰	۹۰۰	۱۰۰۰		

در رمزنویسی با استفاده از حروف ابجد، به جای آنکه کلمات را بنویسند، حروف هر کلمه را می‌نویسند، مطابق اعداد ابجد که در بالا ذکر شد و البته درباره حروف فارسی که در ابجد نیست، عدد مشابه آن نوشته می‌شود؛ یعنی «پ» را مثل ب(۲)، «چ» را مثل جیم(۳)، «ژ» را مثل زاء(۷) و گاف را مثل کاف(۲۰) می‌نویسند. همزه معمولاً به حساب نمی‌آید؛ ولی گاهی آن را معادل الف (۱) می‌گیرند و در تمام موارد، صورت مکتوب مراعات می‌شود نه ملفوظ؛ مثلاً

مرتضی را با یای حساب می‌کنند نه با الف و «تا»ی گرد برابرهای گرد است. (ذاکری، ۱۳۸۸: ۱۲۳)

هر چند اطلاعات چندانی از مکاتبات رمزی در دوره صفوی تا قاجار، به دلیل دسترسی نداشتن یا موجود نبودن سندی در این خصوص، نیست، اما در *خزاین ملاحمد نراقی* و به شکل کامل‌تر در *تحفه المومنین اقلامی* ذکر شده که به نظر می‌رسد این اقلام در مکاتبات رمزی آن دوره‌ها مورد استفاده قرار می‌گرفته است. در *خزاین ملاحمد نراقی* به چند نوع از اقلام رمزی اشاره شده است که از آن جمله می‌توان به قلم مراد به ترتیب ابنت، قلم اسراف، قلم طبیعی، دو نوع قلم یونانی، قلم زهره و مشتری، قلم قمر، سه نوع قلم عطارد، قلم اوسراس حکیم که به قلم طبیعی مشهور است، قلم قلیسپین نوش حکیم، قلم سرمانوس حکیم، قلم ریحان و قلم کاشفی. (نراقی، ۱۳۰۸ق: ۲۶۵-۲۶۴) در کتاب *تحفه المومنین* نیز چند نوع قلم، کامل‌تر از آنچه در *خزاین* است، آمده؛ این کتاب «اقسام مشهوره خطوط مرموزه» را شامل دو نمونه (نوع) قلم هندی، قلم برناوی پنج قسم، قلم یونانی دو قسم، عبرانی شش قسم، قلم الاحجار، قلم رومی، قلم شاناق، قلم فرنگی، قلم به ترتیب ابجد لوط، قلم پهلوی، قلم قلقطیر بابلی، قلمی به حروف تهجی جهت حل عقود مجرب، قلم قلقطیر صغیر، قلم کاهی، قلم صینی، قلم جابر بن حیان، قلم حمیمی، قلم ارما بوی، رملی مقطع، تحلیل، رومی، مشجر دیسقوردیدوس، سیمیای کبیر، سیمیای صغیر، العقول، الصابی، داودی، اسماعیلی، جعفری، الاسرار، قلم حمیری، مشجر یا سروک و چند نمونه دیگر از خطوط رمزی دیگر به صورت تهجی ذکر کرده و نمونه اقلام مذکور را نیز آورده است. (حکیم مومن، ۱۲۹۰ق: ۳۲۲-۳۱۹)

این اقلام متشکل از اشکال مختلف به جای حروف یا ترکیبی از اشکال و حروف ابجد است و تاریخ اختراع یا میزان بهره‌بردن از این اقلام نیز، با توجه به نبود یا کمبود منابع سندی در این خصوص به درستی روشن نیست. در منابع ذکر شده نیز تنها به نام اقلام، ترسیم اشکال و کلید آنها اکتفا شده است. در بین این اقلام، قلم مشجر (شجری) بسیار استفاده می‌شده است. این قلم براساس حروف ابجد بوده و به دلیل شباهتش به درخت، به خط یا قلم شجری معروف شده است. خط عمودی و خطوط مایل شاخه‌گونه در طرفین، نشانه حروف آن است. هر حرف شجری یا هر درخت از نظم خاصی پیروی می‌کند؛ شاخه سمت راست، غیر از حروف کلمه ابجد، نشانه کلمه و شاخه سمت چپ نشانه حرف است. در حروف ابجد هیچ شاخه‌ای در طرف راست نیست و این نشانه کلمه ابجد است و به ترتیب از حرف اول تا چهارم از یک تا چهار شاخه در طرف چپ قرار دارد. در حروف هوز یک شاخه در طرف راست نشانه کلمه هوز و شاخه‌های طرف چپ نشانه «ه و ز» است و به همین ترتیب تا آخرین حرف این نظم برقرار است. (کسای، ۱۳۸۷: ۱۹۷-۱۹۵)

رمزنگاری نوین

امروزه رمزنگاری یکی از شاخه‌های ریاضی، علوم کامپیوتر و مخابرات محسوب می‌شود. در طی قرون نوزدهم و بیستم میلادی، اروپاییان فعالیت‌های جدیدی را در حوزه رمزنگاری آغاز کردند و ماشین‌های رمز پیشرفته‌ای را تولید و عرضه کردند. از جمله معروف‌ترین این ماشین‌های رمز، ماشین رمز انیگما بود که فردی آلمانی به نام آرتور شریبوس آن را در سال ۱۹۱۸م طراحی کرد و ساخت. این ماشین در آن زمان آن قدر پیچیده بود که اکثر ریاضی‌دانان و رمزنگاران آن دوره فکر می‌کردند حتی تلاش برای شکستن رمزهای تولیدی آن کار بیهوده‌ای است. (شیری، ۱۳۹۳: ۲۹) با پیشرفت علم و ظهور کامپیوترها شیوه‌های جدید در رمزنگاری ابداع شد و سیستم‌های رمز دیجیتال به سرعت در صنعت رمز ظهور پیدا کرد، رمزکننده‌های دیجیتال ساخته شد که در ارتباطات امن به کار گرفته شدند.

ایرانیان نیز تا پیش از دوره قاجار و حتی اوایل این دوره، نیاز چندانی جهت اختراع شیوه‌های جدید برای رمزنگاری احساس نمی‌کردند. اما هر شیوه رمزنگاری تا زمانی کارآمد است که فقط افراد محدودی از رمزگشایی آن آگاه باشند و با ابزار و روش نامه‌نگاری آن دوره مطابقت داشته باشد. هر چند عده‌ای سعی داشتند این نکته را متذکر شوند که رمزهای سنتی قابلیت استفاده در ارسال پیام‌های تلگرافی را دارد؛ هیچ‌گاه در مکاتبات رسمی از این رموز استفاده‌ای نشد. (فانی تبریزی، ۱۳۰۰ ق: ۳-۲) به‌طور کلی ضعف و کارایی نداشتن رمزنگاری سنتی را می‌توان در گزینه‌های زیر خلاصه کرد:

۱. سادگی، تکراری بودن اقلام و شیوه‌های پیشین و نداشتن تلاش رمزشناسان آن حوزه به منظور روزآمد کردن آن: اقلام رمزی متشکل از اشکال و نشانه‌های مختلف بود که با کمی صرف وقت، رمزشناسان آن را رمزگشایی می‌کردند. آنها با آشنایی با قواعد یک زبان و نیز شناخت حروف پربسامد آن می‌توانستند این کار را انجام بدهند. چنانچه در زبان عربی این ترکیب حروف به ترتیب پربسامد هستند: «المونتری»، «عهدک»، «صبح قفس»، «زجش»، «خطط»، «تضدغ» یا در زبان فارسی ترکیب حروف «اردیمون»، «هبتلشسک»، «خنز»، «قحفگ»، «جطص/پچض»، «ذغظژث» به ترتیب پربسامدترین حروف به شمار می‌آیند. (مفتاح‌الملک، ۱۳۲۰ ق: ۴۲ و ۶۳) رمزشناسان در رمزگشایی از روش‌های رمزنگاری با استفاده از حروف ابجد و سایر دوایر حروف نیز، کار سختی پیش رو نداشتند؛ چرا که با برابر هم قراردادن حروف و اعداد مربوط به هر کدام به راحتی می‌توانستند رمز را کشف کنند؛

۲. دشواری استفاده از این گونه اقلام رمزی در ارسال پیام‌های تلگرافی؛ چرا که در بسیاری از این رموز از نشانه‌ها و اشکال مختلف استفاده شده بود؛

۳. برجسته شدن جنبه تفننی رمزنگاری سنتی و در نتیجه عمومی شدن و گسترش فراگیری فنون آن.

اقلام رمزی قائم مقام فراهانی

در این دوره علاوه بر استفاده از اقلام رمزی پیشین، عده‌ای نیز مانند میرزا ابوالقاسم قائم مقام فراهانی به اختراع خطوط رمزی جدیدی دست زدند. نمونه‌هایی از این خطوط رمزی را می‌توان در اسناد دوره قاجار مشاهده کرد. (ساکما، ۲۹۵/۷۴۲۵) از ویژگی‌های عمده خطوط اختراعی وی می‌توان به ترکیب حروف، اعداد، ارقام سیاقی و نیز اشکال دیگر و جانشینی آنها به جای حروف اصلی، تنوع و تعدد این اقلام و بسنده نکردن به یک قلم رمزی، اشاره کرد. اساس اقلام رمزی قائم مقام همان رمزهای پیشین است، اما پرداختن او به این مسئله و تلاش برای ابداع اقلام جدید به منظور پیدا کردن کانالی امن جهت ارتباطات رمزی تا پیش از پیدایش تلگراف در ایران شایسته توجه است.

مفتاح‌الملک در این خصوص به تشریح «خطوط مرموزه» جدید قبل از ایجاد تلگراف (در سده سیزدهم) می‌پردازد که خود او و به دستور ناصرالدین شاه کشف کرده است. «نوشتجات مرموزه بسیار از زمان خاقان جنت مکان فتحعلی شاه طاب ثراه بود که در نزد مرحوم میرزا ابوالقاسم قائم مقام جمع شده بوده است؛ یعنی آن مرحوم که در فضل و دانش و حسن کفایت و کاردانی معروف و فرید عصر خود بوده برای مکاتبات محرمانه با شاهزادگان عظام و وزرا و حکام بزرگ آن زمان مفاتیح عدیده رمز وضع کرده و با هر یک جداگانه مکاتبات مرموزه داشته و پس از گرفتاری آن مرحوم و ضبط نوشتجات او کاغذهای رمز بسیار در میان آنها به دست آمده و ضبط دولت شد و چون مفاتیح آنها در دست نبود در این مدت متمادی لاینحل مانده و در کتابخانه مبارکه دولتی مضبوط بود.» (مفتاح‌الملک، ۱۳۲۰ق: ۲۲) وی اقسام خطوط اختراعی قائم مقام و مفاتیح آنها را پانزده مورد ذکر کرده است. (همان: ۳۱-۲۴)

روز	ق	ك	ك	ل	م	ن	و	ه	ی
روز	،	۴	۵	ل	م	ن	۶	ه	ی
قسمت‌های نهم									
روز	ا	ب	پ	ت	ث	ج	چ	ح	خ
روز	۱	۲	۳	۴	۵	۶	۷	۸	۹
روز	س	ر	س	ش	ص	ض	ط	ظ	ع
روز	ظ	ط	ص	ص	ه	س	ل	م	ا
روز	چ	ك	ك	ل	م	ن	و	ه	ی
روز	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
قسمت‌های دهم									
روز	ا	ب	پ	ت	ث	ج	چ	ح	خ
روز	۱	۲	۳	۴	۵	۶	۷	۸	۹
روز	س	ر	س	ش	ص	ض	ط	ظ	ع
روز	ه	ک	ط	ط	ع	ط	ص	ص	لا

نمونه‌ای از اقلام اختراعی قائم مقام فراهانی همراه با کلید رمز (مفتاح‌الملک: ۱۳۲۰: ۲۹)

رمز یوسفی

تشکیل وزارت امور خارجه در دوره قاجار و آشنایی سفرای اعزامی به خارج با وضع و ترتیب رمز نویسی در سایر کشورها و لزوم ارسال «نوشتجات مخفی» برای مأموران اعزامی به خارج از کشور، عده‌ای را به فکر ترجمه و تألیف کتاب‌هایی در این زمینه انداخت. (بران مرتنس، ۱۳۹۴: ۷۶-۷۴) در ایران اولین کسی که اقدام به تألیف اثر رمزی مناسب به منظور ارسال تلگراف‌های رمز کرد، میرزا یوسف خان مستشارالدوله بود. به همین منظور وی کتاب رمز یوسفی را در سال ۱۲۸۱ق. نوشت. این کتاب مشتمل بر یک مقدمه و ده «بیان» است. در مقدمه به معنی تلگراف و برخی از اصطلاحات تلگرافی، چگونگی نوشتن و ارسال مطالب رمزی با ارقام هندسی، چگونگی مفتاح با سه روش جمع، تفریق و تقدیم (تأخیر) می‌پردازد. (مستشارالدوله، بی‌تا: ۷-۱) وی این کتاب را در زمان مأموریت خود «به جنرال قنصلگری تفلیس و شارژدافری پاریس» از روی رمزهای عددی اروپاییان ترتیب داده و در مقابل هر کدام از کلمات رایج آن دوره، چهار رقم از ارقام هندسی را آورده که هنگام نوشتن رمز، ارقام مقابل هر کلمه را تغییری که معهود

بوده، رمز و به جای کلمات مطلب ارسال می‌کردند و تا «مدتی هم مخابرات مرموزه تلگرافی دولتی با ممالک خارجه از روی آن معمول بوده» است. (مفتاح الملک، ۱۳۲۰ق: ۳۳) در بیان دوم این کتاب مستشارالدوله اشاره می‌کند که این رمز «فزون‌تر از صد هزار مفتاح دارد که هر یک از همان مفاتیح را دو نفر به جهت سد راه پیدا کردن دیگران می‌توانند مابین خود قرار بدهند.» (مستشارالدوله، بی‌تا: ۲) وی در توضیح مفتاح با این رمز به قاعده جمع می‌نویسد: «طرز اول به قاعده جمع است یعنی زاید کردن عددی که مابین دو شخص از سابق قرار داده شده» است، بدین ترتیب که دو فرد متعاقد برای ارتباط رمزی با یکدیگر، ابتدا عددی را انتخاب و معهود قرار داده و به اعداد رمز شده، اضافه کرده و پیام را ارسال می‌کنند. به‌عنوان نمونه اگر مفتاح دو شخص متعاقد عدد ۲۱۴ باشد و قرار آنها عمل جمع باشد، باید این عدد را زیر اعداد رمز شده (استخراج از کتاب رمز یوسفی) نوشته و آن را به اعداد مزبور اضافه کرده، حاصل جمع را به دست آورده، پس از اضافه کردن این عدد به اعداد رمز و ارسال آن، طرف مقابل از هر کدام از اعداد رمز به طور جداگانه ۲۱۴ را کم کرده و ارقام اصلی رمز به دست می‌آید. مثلاً برای ارسال جمله « ایلچی امریکا وارد تهران شدند» ابتدا با استفاده از رمز یوسفی اعداد معادل هر کدام از کلمات را به‌این ترتیب زیر آن نوشته:

ند-شد	تهران	وارد	امریکا	ایلچی
۵۵۱۷-۸۷۱۹	۸۹۳۷	۸۹۹۵	۱۲۳۷	۱۹۱۸

بعد از آن عدد ۲۱۴ را به هر کدام از اعداد بالا اضافه کرده که به ترتیب اعداد ۸۹۳۳-۵۷۳۱، ۶۱۵۱، ۹۲۰۹، ۱۴۵۱، ۲۱۳۲ به دست می‌آید، این اعداد به‌عنوان پیغام رمز ارسال می‌شود و دریافت‌کننده باید عدد ۲۱۴ را از این اعداد کم کرده تا ارقام اصلی به دست آمده و با مراجعه به کتاب رمز یوسفی پیغام را کشف کند. طرز دوم به قاعده تفریق یعنی کم کردن عدد معین و معهود از اعداد رمز شده است. در این روش اگر همان مثال قبلی را در نظر بگیریم، عدد ۲۱۴ را از اعداد رمز کم کرده و بعد از ارسال، طرف مقابل عدد مفتاح یعنی ۲۱۴ را به اعداد می‌افزاید و اعداد اصلی رمز به دست می‌آید و با توجه به رمز یوسفی مطلب را رمزگشایی می‌کند. روش سوم قاعده تقدیم و تأخیر است. در این روش ارقام قبل یا بعد از کلماتی را که به منظور ارسال پیغام رمزی مدنظرند، با استفاده از لغت رمز یوسفی استخراج و ارسال می‌کنند که در این صورت مثلاً برای ارسال مطلبی رمزی با قاعده تقدیم، باید اعداد قبل از هر کدام از کلمات مدنظر برای ارتباط رمزی را از لغت رمز یوسفی استخراج کرده و مطلب را ارسال کرد. (همان: ۷-۵) مستشارالدوله در سال ۱۲۹۲ق. یعنی یازده سال پس از چاپ کتاب اول،

تاریخ‌نگاری و تاریخ‌نگاری، سال ۲۹، شماره ۲۴، پاییز و زمستان ۱۳۹۸ / ۱۷۷

کتاب دوم خود را به دستیاری محمدآقای سرتیپ، برادر محسن خان مشیرالدوله در تبریز به چاپ رسانید. (مفتاح الملک، ۱۳۲۰ق: ۱۰۹)

رمز محمودی

محمودبن یوسف مازندرانی ملقب به مفتاح‌الملک، از معروف‌ترین رمزنویسان دوره قاجار به‌شمار می‌رود. وی برای رمزگشایی بسیاری از رموز «قدیمه» به دریافت لقب و منصب «منشی رموزی و کفالت مطالب و مخابرات محرمانه و مرموزه دولتی» در سال ۱۲۸۶ ق. سرفراز شد. (همان: ۳) او درباره کار خود می‌نویسد: «هر قدر و از هر جا خطوط مرموزه قدیمه و جدیده به دست آمده است، بدون هیچ سابقه و اطلاع از وضع واضح آنها منکشف ساخته و خود نیز انواع رمزها اختراع و وضع کرده و کتاب‌ها در معرفت آنها ترتیب داده که سال‌هاست مخابرات محرمانه و مرموزه دولتی از روی آنها معمول و دایر است.» (همان: ۵) مفتاح‌الملک در کتاب‌های خود انتقادات زیادی را بر شیوه رمزنویسی قدما وارد می‌کند و نوشتن مطالب محرمانه با استفاده از آن‌گونه رمزها را مثل آن می‌داند که «کسی چشم خود را بر هم بگذارد و گمان کند مردم او را نمی‌بینند» و در جای دیگر زحمات آنان را در «استحکام ارقام مرموزه» مثل آن می‌داند که «کسی برای حفظ خانه خود از شر دزد دری آهنین و خیلی محکم بگذارد و قفل‌های عدیده و زنجیرهای سخت در آن به کار ببرد و سنگ‌های عظیم بر پشت آن نصب کند و در کمال اطمینان آسوده‌خاطر بخوابد و دزد آگاه بدون زحمت شکستن قفل‌ها و گسیختن زنجیرها و حرکت دادن سنگ‌ها با نردبان با کمال سهولت از بام داخل خانه شده و آنچه بخواهد ببرد.» (همان: ۶ و ۲۱)

وی بهره‌بردن از ارقام رمزی قدیمی به منظور ارسال تلگراف به «ممالک خارجی» را مناسب نمی‌داند و می‌نویسد: «هرگاه در ازمنه سالفه مطالب محرمانه را با ارقام غریبه و سایر رمزها نوشتند چون آنها در نوشتجات سربسته و مهور و مصحوب قاصد چاپارهای مخصوص و مستور بود و به ممالک خارجه هم نمی‌رفت و به دست خارجی هم نمی‌افتاد چندان محل ملاحظه و احتیاط نبود؛ ولی حالا که مطالب مرموزه را با تلگراف مخیره می‌نمایند و صورت آنها در تمام تلگرافخانه‌های [تلگرافخانه‌های] داخله و خارجه ثبت و ضبط می‌شود و معایب بی‌استحکامی آنها و نتایج وخیمه مترتبه بر آن ظاهر و عیان و مستغنی از شرح و بیان است.» (همان: ۶)

به‌واسطه ممکن نبودن مخابره تلگرافی با ارقام رمزی قدیمی، اقسام جدیدی ایجاد شد تا بتوان از آنها در مخابره تلگراف استفاده کرد که مفتاح‌الملک به تشریح آنها می‌پردازد:

«قسم اول آن است که هر دو نفر برای مخابرات محرمانه مابین خود الفبایی ترتیب داده در مقابل هر حرفی از حروف تهجی یک رقم یا دو رقم از ارقام هندسیه رسم کرده و معهود قرار می دهند که در وقت ضرورت مطالب محرمانه خود را از روی آن مخابره و تلگراف نمایند. قسم دیگر آن است که الفبایی نوشته و در مقابل هر حرفی از آن حرفی دیگر از حروف تهجی یا حروف جمل گذاشته و در وقت ضرورت به جای حروف مطلب مقابل آنها را می نویسند. قسم دیگر آن است که بعضی از حروف تهجی را تبدیل کرده و بعضی دیگر را به حالت خود می گذارند. قسم دیگر آن است که الفبایی به ترتیب ابثی و یا به ترتیب ابجدی و یا هر ترتیب دیگر که بخواهند می نویسند و قرار می دهند که در وقت نوشتن رمز حرفی که لازم شود در آن الفبا پیدا کرده و حرف ماقبل آن و یا حرف مابعد آن را که معهود قرار داده اند، در عوض آن می نگارند. و قسم دیگر رمز یوسفی است.» (مفتاح الملک خود نیز در همین راستا دست به اختراع انواعی از اقلام رمزی مانند رمز رحوی، فلکی، ثنائی زد). (همان: ۳۵-۳۲)

وی بعد از اینکه هیچ کدام از خطوط رمز را شایسته برای «مخابرات مرموزه دولتی» ندید، در سال ۱۲۹۹ق. کتاب *ناسخ الرموز* را نوشت که در مکاتبات رمزی تلگرافی استفاده شد. در این کتاب، با رعایت «ترتیب حروف، کلمات مفرده و مرکبه کثیر الاستعمال از اسامی، افعال و ضمائر و کلمات و اصطلاحات خارجی» که در نوشتجات و مخابرات تلگرافی لازم می شد، به ترتیب حروف تهجی به صورت ثلاثی (سه حرفی) آورده شده است. حروف استفاده شده مفتاح الملک در این کتاب رمز، مرکب از بیست و پنج حرف است و بنا به «ملاحظات لازمه» از حروف فارسی (پ چ گ ژ) و حروف (ت ث ف)، استفاده نکرده است. (مفتاح الملک، ۱۳۱۹ق: ۱۲)

س	ز	ر	ذ	د	خ	ح	ج	ب	ا
م	ل	ک	ق	غ	ع	ط	ض	ص	ش
						ی	ه	و	ن

برای رمزکردن مطلبی با استفاده از حروف تهجی و با توجه به کتاب *ناسخ الرموز*، ابتدا میان دو طرف کلید رمزی ترتیب داده می شد، به این ترتیب که به جای هر یک از بیست و پنج حرف انتخاب شده، حرف دیگری قرار داده و طرفین، نسخه ای از آن را نزد خود نگاه می داشتند و هنگام مخابره تلگراف، حرفی را که در کتاب رمز، مقابل کلمات نوشته بودند، به حروف کلید تبدیل می کردند. برای استخراج پیام رمز شده، طرف مقابل از روی کلید مزبور که نسخه ای از آن را در اختیار داشت، این حروف را به حروف اصلی برمی گرداند و از روی لغت

تاریخ‌نگری و تاریخ‌نگاری، سال ۲۹، شماره ۲۴، پاییز و زمستان ۱۳۹۸ / ۱۷۹

ناسخ‌الرموز، مطلب را استخراج می‌کرد. (همان: ۱۵-۱۴؛ ساکما، ۳۹۷۱۷/۲۴۰) برای ارسال تلگراف‌های رمز به خارج از کشور نیز چون حروف فارسی کاربرد نداشت، از حروف لاتین استفاده (از چپ به راست) و سپس پیام را ارسال می‌کردند. به همین منظور اشخاصی که قصد ارسال تلگرافی به خارج از کشور را داشتند، باید مفتاحی را معهود قرار می‌دادند که حروف رمز ثلاثی به «حروف فرنگی» باشد و در نوشتن هم از سمت چپ بنویسند تا در تلگراف‌خانه‌ها اشتباهی روی ندهد. (همان: ۱۶) مثلاً اگر بین دو نفر کلید تبدیل حروف رمز ثلاثی به حروف فرنگی به این ترتیب باشد:

ض	ص	ش	س	ز	ر	ذ	د	خ	ح	ج	ب	ا
m	n	l	k	j	i	h	g	f	e	c	t	a
ی	ه	و	ن	م	ل	ک	ق	ع	ع	ظ	ط	
d	b	z	y	x	v	u	s	r	q	p	o	

و بخواهند مطلب زیر را به رمز بنویسند:

«تلگراف رمز شما رسید، مطلب خیلی مفصل و لازم بود، واقعاً اگر می‌خواستند این مطلب عمده را با سایر رمزها تلگراف بکنید مبلغی گزاف اجرت تلگراف می‌شد، به دست خارجی هم که می‌افتاد مطلب آن را می‌فهمید اما حالا که با کتاب ناسخ‌الرموز نوشته‌اید، هم اجرت تلگراف خیلی کم شده است و هم بدون مفتاح احدی از این مطلب مطلع نخواهد شد»، ابتدا باید کلمات و عبارات این مطلب را در کتاب ناسخ‌الرموز پیدا کرده و حروف برابر هر کدام را در زیر آن نوشت.

۱۸۰ / رمزنگاری در دوره قاجار؛ گذر از رمزنگاری ستی به رمزنگاری نوین / صمد کاوسی رکعتی

واقعاً	لازم بود	و	خیلی مفصل	مطلب	تلگراف رمز شما رسید
وظل را	غسض عمده	وضق	ساد	کسح	یمر
سنغ	طقش	کسح	جظه	لوض	بول
می شد	مبلغی گزار اجرت تلگراف	تلگراف کنید	رمزها	سایر	با
مخد	یکو	دضع	شرد	صاح	جعو
مطلب	می افتاد	که	هم	خارجی	بدست
کسح	لظی	عوس	هده	زح	حشس
کتاب	با	حالا که	اما	می فهمید	آن را
عرق	جعو	رقس	جاج	مرخ	اسش
وهم	خیلی کم شده است	اجرت تلگراف	هم	نوشته اید	ناسخ الرموز
هخ	یقن	اعط	هده	وزش	مضص
		نخواهد شد	احدی از این مطلب مطلع	مفتاح	بدون
		می	یذع	کغش	حصخ

سپس با استفاده از کلید ذکر شده حروف را به لاتین تبدیل کرده و به ترتیب ذیل برای طرف مقابل ارسال کرد. (همان: ۹)

ابداً

xid	eku	gak	snz	nkr	vpz
vzt	nzv	bpc	ekul	so	ryk
zgc	eam	hil	gmh	zud	gfx
kbe	yej	egb	kzq	dpr	eku
lka	fix	rac	ksi	zgc	siq
mnal	jz	egb	oga	y sd	fab
fme	lru	ghd	dbx		

مفتاح‌الملک در همین نسخه ناسخ‌الرموز چاپ ۱۳۱۹ق.، به قانون جدید تلگراف‌خانه‌های خارجی اشاره می‌کند که قبل از آن هر سه حرف از حروف رمز یا سه رقم از ارقام هندسی را که متصل و بلافاصله نوشته می‌شدند، یک کلمه تلگرافی محسوب می‌کردند و اگر با فاصله می‌نوشتند، هر یک حرف یا یک رقم را یک کلمه حساب می‌کردند. به همین دلیل بود که مفتاح‌الملک هم ترتیب رمز را، ثلاثی یعنی سه حرفی قرار داد که مطابق با قانون معمول تلگراف‌خانه‌های خارجی باشد. وی با اشاره به اینکه از پنج سال قبل، مطابق با ۱۳۱۴ق.، قانون عمومی تلگراف‌خانه‌های خارجی بر این قرار گرفت که هر پنج حرف رمزی را که متصل و بلافاصله نوشته شده باشند، یک کلمه محسوب کنند؛ بنابراین «ما هم موقع را برای تحصیل صرفه مجدد مغتنم دانسته قرار مخابرات مرموزه خودمان را با ممالک خارجه به این طور دادیم که در وقت مخابره تلگرافی هر سه کلمه رمز خودمان را که عبارت از نه حرف است متصل و بلافاصله بنویسیم که در این صورت در تلگراف‌خانه‌های خارجه این سه کلمه رمز ما را که نه حرف است دو کلمه محسوب دارند، پس از این بابت هم یک ثلث علاوه بر صرفه سابق صرفه مجدد برای ما حاصل شده است.» (همان: ۲۴۷)

پیش از این و در سال ۱۳۱۳ق. مفتاح‌الملک «چون در مخابره مطالب مرموزه تلگرافی با ممالک خارجه و ولایات داخله، در تلگراف‌خانه‌های داخله و خارجه بلکه از طرف اغلب نویسندگان رمزها هم به‌طوری که لازم است، اهتمام و دقت کامل نمی‌شود و مقابله و تصحیح صحیح چنان که باید به عمل نمی‌آید، لهذا غالباً مطالب مرموزه تلگرافی مغلوط می‌شود»، اقدام به نوشتن کتاب *کشف الاسرار ناصری* با هدف رفع این «اشکالات و محظورات» کرد. (مفتاح‌الملک، ۱۳۱۳ق: ۴-۳) در این کتاب علاوه بر سه باب کتاب *ناسخ‌الرموز*، دو باب دیگر هم به ترتیبی خاص افزوده که وضع و ترتیب فصول آن همانند وضع و ترتیب فصول باب دوم و سوم کتاب *ناسخ‌الرموز* است؛ اما در اینجا به جای رمزهای ثلاثی یعنی سه حرفی، در مقابل اسامی ماه‌ها، اعداد، واحدهای پولی، اوزان و اصطلاحات، لغت و کلمه‌ای مخصوص از قبیل اسامی شهرها و اشخاص و غیره به‌صورتی که خود تشخیص داده، وضع کرده و آن کلمه یا عبارت را به خط فرانسوی هم نوشته تا در صورت «مخابره با ممالک داخله» و استفاده از خط فارسی، همان لغت را با خط فارسی به جای آن کلمه یا عبارت و در صورت مخابره به خط فرانسوی آن لغت را هم به خط فرانسوی در مقابل آن کلمه، عیناً و بدون نیاز به رمزشدن نوشته شود. (همان: ۵-۴)

<i>Aboutaleb</i>	ابوطالب	شهر چهارم ثانیة
<i>Oporto</i>	اُبْرُتُ	شهر حجاب المرجب
<i>Atabek</i>	اَنَابُک	شهر شعبان العظم
<i>Etalle</i>	اِشَال	شهر رمضان المبارک
<i>Atane</i>	اَتَان	شهر شوال الکفر
<i>Atrek</i>	اَنُرُک	شهر ذیقعده الحرام
<i>Autriche</i>	اُتْرِش	شهر ذیحجه الحرام

فَضْلُومِ کَرَامَتِ هَارُونِ

<i>Attique</i>	اَتِیک	نشین اول
<i>Ahmed</i>	اَحْمَد	نشین آخر
<i>Akhal</i>	اَخَال	کانون اول

<i>Contra</i>	سَنُورَا	از سفارت در این باب اظهار کرده
<i>Sindjab</i>	سَنَجَاب	از سفارت کبرای دولت
<i>Singueledj</i>	سَنَکَلِج	از تغییر اذنان ملک خود نان اطلاع میداد
<i>Sinandedj</i>	سَنَنَدِج	اسباب اغتشاش کرده شده است
<i>Suez</i>	سُوْشُر	استخراج نلکرا از فرستادن اجناس عالی ^{بسیار}
<i>Souti</i>	سُوْی	افدامان عماد در خاک و تبارک و تعالی ^{بسیار}
<i>Soudan</i>	سُوْدَان	افدامان لازم بعمل آمده است
<i>Suffolk</i>	سُوْفُلْک	افدامان لازم بعمل نیاوردید
<i>Suhla</i>	سُوْهَلَا	اگر این کارها تمام کردید
<i>Suisse</i>	سُوِیس	امر به مقروض بودن
<i>Sohrab</i>	سُوْرَاب	اولیای دولت علیته
<i>Siam</i>	سِیَام	بیتوجه مذاکرات لازم خواهد شد

تاریخ‌نگری و تاریخ‌نگاری، سال ۲۹، شماره ۲۴، پاییز و زمستان ۱۳۹۸ / ۱۸۳

در سال ۱۳۰۲ شمسی، مفتاح الدوله پسر مفتاح‌الملک، *ناسخ‌الرموز* را تجدید چاپ کرد و در آن از جزوه مهدی صلحی، ناظم‌الحکما، نیز استفاده کرد که شامل لغاتی جدید بود و در تبریز در سال ۱۳۰۰ ش. چاپ شده بود. در سال ۱۳۱۰ ش. وزارت جنگ در نامه‌ای به ریاست وزرا، *ناسخ‌الرموز* را برای «مخابرات رمزی آن وزارتخانه» به دلایل محدود نبودن مطالب رمزی قشونی، اتلاف وقت و نداشتن جملات و کلمات ضروری و لغات لازم در مخابرات پیام به اروپا، ناکافی می‌داند و در ادامه از ریاست وزرا درخواست می‌کند که با توجه به اینکه طبع و فروش کتاب رمز به اسماعیل‌خان عاشوری متصدی ملزومات وزارت امور خارجه اختصاص دارد، نواقص کتاب را رفع کند. اما وزارت امور خارجه ادعای وزارت جنگ درباره اختصاص طبع و فروش *ناسخ‌الرموز* به عاشوری را رد و در ادامه بر فروش امتیاز کتاب مزبور از سوی مفتاح الدوله به وزارت مالیه در سال ۱۳۰۲ تأکید می‌کند. (ساکما، ۳۱۰/۳۱۰۹۸) سرانجام *ناسخ‌الرموز* پس از چند بار تجدید چاپ، بار دیگر در سال ۱۳۱۱ ش. با تشکیل کمیسیونی از وزارتخانه‌های مختلف در وزارت جنگ، پس از اصلاحاتی، تجدید چاپ شد تا دوباره تلگرافخانه‌ها برای ارسال مطالب رمز از آن استفاده کنند (ساکما، پایگاه فارس، ۹۸/۲۹۳/۱۱۲۳؛ ساکما، ۲۴۰/۷۵۶۴۷؛ ۲۹۳/۵۴۹۲۳) بعد از تشکیل فرهنگستان زبان فارسی نیز لغات جدید به آن افزوده شد و در تلگراف‌های رمز تا مدت‌ها و تا قبل از تحولات جدید در رمزنگاری، تلگراف‌کنندگان داخل و خارج از کشور از آن استفاده می‌کردند.

نتیجه‌گیری

ارتباطات رمزی از زمان‌های دور رایج بوده و بشر در ابتدا برای ارسال پیام‌های رمزی از علائم و نشانه‌ها بهره می‌برده است. بعد از اختراع خط، بشر توانست با تغییر یا تبدیل حروف و اعداد برای ایجاد کانالی امن در راستای ارتباطات رمزی سود ببرد. در بیشتر تمدن‌های باستانی جهان مانند ایران، شواهد و اشاراتی از وجود چنین خطوط رمزی موجود است. در ایران بعد از اسلام اطلاعات بیشتری در این زمینه وجود دارد، در این دوره در رمزنگاری که بیشتر به تعمیمه یا معماسازی معروف بود، مانند سایر مسلمانان از روش‌های مختلفی مانند جابه‌جایی حروف، کاستن یا افزودن بر حروف و البته حروف ابجد استفاده می‌شده است که کاربرد بیشتری داشته است. در دوره معاصر نیز کسانی مانند قائم مقام فراهانی دست به اختراع اقلام رمزی جدیدی زدند که البته به نظر می‌رسد بعد از خود وی، دیگر کاربردی نداشته است. استفاده از اقلام رمزی قدیمی به دلیل سادگی و آسان بودن رمزگشایی از این اقلام و نیز مشکلاتی نظیر ترکیب حروف و ارقام و اشکال، به‌خصوص در مخابرات پیام‌های تلگرافی امر دشواری بود. بنابراین

عده‌ای در صدد برآمدند تا با توجه به رمزنگاری اروپاییان در مکاتبات محرمانه تلگرافی، کتاب‌هایی را در این زمینه به نگارش درآورند که از مهم‌ترین این کتاب‌ها، می‌توان به کتاب رمز یوسفی نوشته یوسف‌خان مستشارالدوله اشاره کرد. این کتاب مبتنی بر رمزنگاری عددی بود که تا چندی در مکاتبات رمزی تلگرافی استفاده شد. اما بار اصلی در این راه را محمودخان مفتاح‌الملک از رجال دوره ناصری بر دوش کشید. مفتاح‌الملک با نوشتن کتاب *ناسخ الرموز* که رمزی حروفی بود، مدتی طولانی یکه‌تاز میدان رمزنگاری در دوره قاجار و پهلوی شد، به طوری که این کتاب بعد از چند بار تجدیدنظر و چاپ، مهم‌ترین مرجع وزارتخانه‌های دولتی در زمینه ارسال پیغام‌های رمزی به حساب می‌آمد و از اعتبار شایان توجهی برخوردار بود. رمز مزبور که به رمز محمودی نیز مشهور است، به صورت ثلاثی بوده و علاوه بر سادگی استفاده از آن، بعد از انتخاب کلید مدنظر، از لحاظ مالی نیز برای ارسال‌کنندگان بسیار به صرفه بود. بنابراین مفتاح‌الملک با آگاهی از ضعف سایر اقلام رمزی و به‌خصوص در ارسال تلگراف‌های محرمانه به خارج از کشور، موفق به اختراع رمزی شد که جهت ارسال این‌گونه پیغام‌ها در داخل و خارج از کشور، اعتبار بسیاری داشت و رمزگشایی آن بدون کلید کار دشواری بود، و این اعتبار آن موجب دوام استفاده از آن در دستگاه‌های دولتی و مأموران سیاسی ایران در خارج و ایجاد کانالی امن در ارتباطات رمزی شد.

کتاب‌شناخت

اسناد

سازمان اسناد و کتابخانه ملی ایران (ساکما)، اسناد شماره ۳۱۰/۳۱۰۹۸، ۲۴۰/۳۹۷۱۷، ۲۴۰/۷۵۶۶۷، ۲۹۵/۷۴۲۵، ۲۹۳/۷۳۲۰، ۲۹/۵۴۹۲۳.

_____، پایگاه فارس، سند شماره ۹۸/۲۹۳/۱۱۲۳.

نسخ چاپ سنگی

فانی تبریزی، اسماعیل بن محمد صادق (۱۳۰۰ ق) *بدایع العلوم کنز الرموز فی علم الفنون*، سازمان اسناد و کتابخانه ملی ایران، شماره دستیابی ۶۹۶۸۶.

مازندرانی، محمود بن یوسف (مفتاح‌الملک) (۱۳۱۳ ق) *کشف الاسرار*، سازمان اسناد و کتابخانه ملی، شماره دستیابی ۶-۱۶۳۶۹.

_____ (۱۳۱۹ ق) *ناسخ الرموز و رمز محمودی*، سازمان اسناد و کتابخانه ملی، شماره

دستیابی ۶-۲۳۱۲۷.

_____ (۱۳۲۰ قمری) *مفتاح الرموز*، چاپ سنگی، سازمان اسناد و کتابخانه ملی،

شماره دستیابی ۶-۱۴۰۶۹.

محمد مؤمن بن محمد زمان (حکیم مومن) (۱۲۹۰ ق) *تحفه المومنین*، سازمان اسناد و کتابخانه ملی، شماره

دستیابی، ۶-۱۸۸۰۱.

تاریخ‌نگری و تاریخ‌نگاری، سال ۲۹، شماره ۲۴، پاییز و زمستان ۱۳۹۸ / ۱۸۵

مستشارالدوله، یوسف‌بن کاظم (بی‌تا) رمز یوسفی، چاپ سنگی، سازمان اسناد و کتابخانه ملی، شماره دستنویابی ۶-۵۰۳۳.

نراقی، ملااحمد (۱۳۰۸ ق) خزائن، چاپ سنگی، سازمان اسناد و کتابخانه ملی، شماره دستنویابی ۶-۲۶۴۳۶.

کتاب‌ها

ابن ندیم، محمدبن اسحاق (۱۳۸۱) الفهرست، مترجم و محقق: محمدرضا تجدد، تهران: اساطیر. اسماعیل‌پور، جمشید (۱۳۸۹) آلبوم خط و نشانه‌های باستان، تبریز: احراز. شیخ‌زادگان، جواد (۱۳۸۹) رمزشناسی مقدماتی، تهران: پژوهشکده پردازش هوشمند علائم. شیرینی، مینا (۱۳۹۳) مقدمه‌ای بر رمزنگاری: از رمزنگاری کلاسیک تا رمزنگاری کوانتومی، تهران: دانشیاران ایران.

صفری ممقانی، عیسی (۱۳۹۶) حروف رمزی در فرهنگ و تمدن ایران، تهران: پایزنه. کشوری، ارسلان (۱۳۸۴) کله‌سر، چاپ ۲، تهران: جهان‌تاب. محمودی، نرگس (۱۳۸۹) رمزنویسی و گویش‌های رمزی، تهران: خیام آزمون، علوم پارسی. مرتنس، بران (۱۳۹۴) قوانین السفر (رساله‌ای در باب آداب دیپلماسی زمانه قاجار)، مترجم: میرزا ابراهیم ملکم، به کوشش صبح خسروی‌زاده و فاطمه امیری پری، تهران: مهاجر. ملکان سرشت، محمد (۱۳۸۱) طالع بینی آریایی، تهران: نذیر.

مقالات

ذاکری، مصطفی (۱۳۸۸) «ابداع خطوط رمزی در فرهنگ اسلامی و ایرانی»، آینه میراث، شماره ۴۵، پاییز و زمستان.

عالم‌زاده، هادی (۱۳۹۰)، «رمزنگاری در نامه‌ها» در صبح الأعشی فی صناعه الإنشاء، ابوالعباس احمدبن علی قلقشندی (۶۵۷-۸۲۱ق)، نامه بهارستان، سال ۱۲، شماره ۱۸ و ۱۹، بهار و تابستان کسای، سیدعلی (۱۳۸۷) «خط شجری»، آینه میراث، شماره ۴۲، پاییز محمدی فشارکی، محسن و مریم شیرانی (۱۳۹۰) «خط معما؛ پژوهش در انواع و شیوه‌های رمزنگاری منشآت»، متن‌شناسی ادب فارسی، شماره ۱۱، پاییز

List of sources with English handwriting

Documents

- (SAKMA), 310/31098; 240/39717; 240/75647; 295/7425; 293/7320; 29/54923
- (SAKMA), Fars Station, 98/293/1123.

Manuscripts [In Persian]

- Fānī Tabrīzī, Esmā'īl b. Moḥammad Ṣādiq (1300), *Badāyi' al-'Olūm Kinz al-Romū fi 'Elm al-Fonūn*, SAKMA, 6-9686.
- Māzandarānī, Maḥmūd b. Yūsif (Miftāḥ al-Molk) (1313), *Kaṣf al-Asrār*, SAKMA, 16369-6.
- Māzandarānī, Maḥmūd b. Yūsif (Miftāḥ al-Molk) (1320), *Miftāḥ al-Romūz*, Litographed, SAKMA, 14069-6.
- Māzandarānī, Maḥmūd b. Yūsif (Miftāḥ al-Molk) (1319), *Nāsik al-Romūz va Raz-e Maḥmūdī*, SAKMA, 23127-6.
- Moḥammad Momin b. Moḥammad b. Moḥammad Zamān (Ḥakīm Momin) (1290), *Toḥfat al-Mominīn*, SAKMA, 18801-6.
- Mostaṣār al-Dolla, Yūsif b. Kāzim, *Ramz-e Yūsifi*, Litographed, SAKMA, 5033-6.
- Narāqī, Mollā Aḥmad (1308), *ḳazān*, Litografed, SAKMA, 6-26436.

Books

- Esmā'īlpūr, ḵamṣīd (1389 Š.), *Ālbum-e ḳaṭ va Niṣānahā-ye Bāstān*, Tabriz: Aḥrār. [In Persian]
- Ibn Nadīm, Moḥammad b. Eshāq (1381 Š.), *Al-Fihrist*, Translated and edited by Moḥammad Reżā Tajaddod, Tehran: Asāṭir. [In Persian]
- Kīṣvarī, Arsalān (1384 Š.), *Kala Sar*, Tehran: jahāntāb. [In Persian]
- Maḥmūdī, Nargis (1389 Š.), *Ramznivisī va Gūyishā-ye Ramzī*, Tehran: ḳayyām Āzlūn, 'Olūm-e Pārsī. [In Persian]
- Malikān Sīrīšt, Moḥammad (1381 Š.), *Ṭāli 'bīnī-e Āryāū*, Tehran: Naḍīr. [In Persian]
- Ṣafarī Mamqānī, 'Īsā (1396 Š.), *Horūf-e Ramzī ddar Farhang*, va Tamaddon-e Īrān, Tehran: Pāzīna. [In Persian]
- Ṣaiḳzādīgān, ḵavād (1389 Š.), *Ramzīnāsī-ye Moqadamāī*, Tehran: Peḵūhiṣkada-ye Pardāziš-e Hūšmand-e Alāim. [In Persian]
- Šīrī, Mīnā (1393 Š.), *Moqadamaī bar Ramznigārī: Az Ramznigārī-ye Klasīk tā Ramznigārī-ye Koāntomī*, Tehran: Dānišyārān-e Īrān. [In Persian]

Articles

- Ālimzāda, Hādī (1390 Š.), "Ramznigārī dar Nāmahā", dar Ṣobḥ al-'Aṣā fi Ṣinā'a al-Enṣā Abul Abbās Aḥmad b. 'Alī Qilqašandī 821-657 AH., *Nāma-ye Bahāristān*, 12, No. 18 & 19, Spring and Summer. [In Persian]
- Dākīrī, Moṣṭafā (1388 Š.), "Ebdā'-e ḳoṭūṭ-e Ramzī dar Farhang-e Eslāmī va Īrānī", *Ātīna Mīrāt*, No. 45, Fall & Winter. [In Persian]
- Kasāī, Sayyed 'Alī (1387 Š.), "ḳaṭ-e Ṣajārī", *Ātīna-ye Mīrāt*, No. 42, Fall. [In Persian]
- Mirtīns, Brān (1394 Š.), *Qavānīn al-Ṣofarā (Risāla dar Bāb-e Ādab-e Dīplomāsī-ye Zamāna-ye Qājār*, translated by Mīrzā Ebrāḥīm Malkom, Edited by Ṣobḥ ḳosravīzāda & Fāṭīma Amīrī Parī, Tehran: Mohājīr. [In Persian]
- Moḥammadī Fiṣārakī, Moḥsin; Šīrānī, Maryam (1390 Š.), "ḳaṭ Mo'amā; Peḵūhiṣ dar Anvā' va Ṣivahā-ye Ramznigārī-ye Monṣaāt", *Matnīnāsī-ye Adab-e Fārsī*, No. 11, Fall. [In Persian]

Cryptography in Qajar Period Passing Through the Traditional Cryptography to the Modern One ¹

Samad Kavousi Rakati ²

Received: 2019/04/11

Accepted: 2020/05/28

Abstract

There have been encrypted connections among human societies for sending confidential messages a long time ago. In the history of Iran also many encryption lines have been used by crypto-writers. With the telegraph introduction, the old encryption lines were out of use. by the invention of new lines, they got used in confidential conversations and reports. This research's central question is to find how the former lines got removed, and Iranian crypto-writers invented the new ones. This research aims to view Iranian crypto-writers' attempts to find a solution for encryption connections through a security canal in Qajar periods. In this research, we have used library resources, especially lithography books and documents. The use of developmental encryption in encrypted connections, especially in telegraph, resulted from the extending political and economic relationship with the western world and being familiar with the modern west cryptography and finding the simple usage rather than the traditional one in the Qajar period. Hence, some Iranian crypto-writers made new encrypted lines with the necessary assurance for sending the internal and external encrypted messages.

Keywords: Encryption, Cryptography, Modern cryptography, Historic documents, Qajar period

1. DOI: 10.22051/HPH.2020.32381.1456

2. MA in History of Islamic Iran, Tehran University, Document Experts in The National Archive & Library of I.R.I (Islamic Republic of Iran); kavousiarad98@yahoo.com

Print ISSN: 2008-8841/ Online ISSN: 2538-3507