دو فصلنامهٔ علمی تاریخ‌نگری و تاریخ‌نگاری دانشگاه الزهرا (س)
سال بیست و نهم، دورهٔ جدید، شمارهٔ ۲٤، پیاپی ۱۰۹، پاییز و زمستان ۱۳۹۸/ صفحات ۱۸۷-۱٦٥
مقاله علمی ـ پژوهشی

رمزنگاری در دورهٔ 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 پدیدآمدن 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 ازطریق کانالی امن در دورهٔ قاجار، پاسخ داده شود. نتیجهٔ این پژوهش نشان می‌دهد که در دورهٔ قاجار به‌دلیل 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، دورهٔ قاجاریه، اسناد تاریخی

---

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

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

مقدمه

رمز کلمه‌ای عربی است از مصدر مجرّد، باب فَعَلَ یَفعُل که در زبان فارسی بسیار کـاربرد دارد. رمز یعنی به لب، چشم، ابرو یا به دهان و زبان اشاره کردن. این واژه به معانی دیگـری نیـز بـه کار رفته است: اشاره، رمز، سرّ، ایما، دقیقه، نکته، معمّا، نشانه، اشارهٔ پنهان، نـشانهٔ مخـصوصی که از آن مطلبی درک شود، چیز نهفته میان دو یا چند کس کـه دیگـری بـر آن آگـاه نباشـد و مقصود با نشانه‌ها و علائم قراردادی و معهود بیان شود. آنچه در تمام این معانی مشترک اسـت صریح‌نبودن و پوشیدگی است. (مفتاح‌الملک، ۱۳۱۳ق: ۱۱۵؛ شیخ‌زادگان، ۱۳۸۹: ٦ ؛ محمـدی فشارکی و دیگران، ۱۳۹۰: ۱۱۸) رمزنگاری، معادل واژهٔ کریپتوگرافی انگلیسی اسـت و از واژهٔ کریپتوس مشتق شده است و موضوع آن پرداختن به مباحث و مسائل مرتبط با تبـدیل پیغـامی آشکار (اصلی) به پیغامی رمزی با استفاده از روش و الگوی مشخص(الگوریتم) و یک یا چنـد کلید است. (شیخ‌زادگان، ۱۳۸۹: ٦) رمزنگاری نزد مسلمانان به تعمیه یا معماسازی مشهور بوده و از روش‌های مختلفی برای ارسال پیغام رمز استفاده می‌کردند. درخصوص موضوع بحث‌شده در این پژوهش تحقیق مستقلی صورت نگرفته است، اما دربـارهٔ رمزنگـاری در متـون قـدیمی به‌خصوص پیش از قاجار نویسندگان، نه از منظر تاریخی، بلکه ادبی و نیز کاربرد رمز در علوم غریبه به این موضوع پرداخته اند و کتاب ها و مقالات و مدخل هایی نیز بـه نگـارش درآمـده است، ازجمله:

کتاب *اسرار و رموز اعداد و حروف* نوشتهٔ احمد آقاشریف که در این کتاب به تاریخچـه و شرح رابطهٔ حروف و اعداد و تقدس آنها پرداخته است. *کله سر* تـألیف ارسـلان کـشوری کـه مخفف پنج کلمهٔ کیمیا، لیمیا، هیمیا، سیمیا و ریمیا است و در این کتاب به شـرح علـوم سِـری پرداخته شده و نیز تقدس حروف و اعداد و چگونگی رمزنویسی با حروف جمل را شرح داده است. *رمزنویسی و گویش‌های* رمزی، نوشتهٔ نـرگس محمـودی کـه در آن بـه تاریخچـه‌ای از رمزنگاری در دنیا و نیز مختصری از شیوه‌های رمزنگاری و رمزگشایی و نیز زبان‌هـای رمـزی اشاره شده است. *حروف رمزی در فرهنگ و تمدن ایران* تألیف عیسی صفری ممقـانی کـه بـه کلیاتی از تاریخ رمزنگاری و شیوه‌های آن تا دورهٔ معاصر پرداخته شده است. مقاله‌های «ابـداع خطوط رمزی در فرهنگ اسلامی و ایرانی» از مصطفی ذاکری، «رمزنگاری در نامه‌ها (برگرفتـه از صبح الأعشی فی صـناعة الإنـشاء قلقـشندی)» از هـادی عـالم‌زاده کـه در واقـع شـرحی از شیوه‌های رمزنگاری مسلمانان از زبان ابن‌دریهم رمزنگار معروف است، «خط شجری» از سـید علی کسایی که در این مقاله شیوهٔ رمزنویسی با خط شجری آمده است، خط معما (پژوهش در انواع و شـیوه‌هـای رمزنگـاری *منـشآت)* از محـسن محمـدی فـشارکی و مـریم شـیرانی کـه

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 دورهٔ قاجار به منظور پدیدآوردن اقلام رمزی جدید در ارتباطات رمزی و محرمانه، سعی دارد به چرایی نادیده‌گرفتن اقلام رمزی سنتی و چگونگی اختراع اقلام جدیدِ این رمزشناسان پاسخ دهد.

رمزنگاری سنتی و پیشینهٔ 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، ۱۳۹٦: ٥٦) 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 علاوه‌بر 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. دانستنِ علم حروف و اعداد از ضروریات علوم غریبه بوده است. (کشوری، ۱۳۸٤: ۲۳٤-۲۳۳)

در چین از خط اندیشه‌نگار که ترکیبی از واژه‌ها و نمادها بود، برای رمزنویسی کمک می‌گرفتند(محمدی فشارکی، شیرانی: ۱۱۱) خط نسیبیدی(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: ۱۸۵-۱۸٤) 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 جولیوس سزار رمز دیگری بود که رومیان استفاده می‌کردند. این رمزنگاری ساده‌ترین رمز جانشینی بود که در آن تمامی حروف به میزان یک گام مشخص جابه‌جا می‌شدند.(شیری، ۱۳۹۳: ۱۷)

در خصوص رمزنگاری در ایران پیش از ساسانیان اطلاعات چندانی در دست نیست. در *الفهرست* ابن ندیم و به نقل از ابن مقفع، ایرانیان پیش از اسلام دارای هفت نوع خط بوده‌اند، ازجملهٔ این خطوط که هر کدام را جداگانه شرح می‌دهد، می‌توان به دین دفیریه، ویش دبیریه، کشتج، نیم کشتج، شاه دبیریه(خط مخصوص مکاتبات شاهان) وهام دبیریه(خط ویژهٔ تمام طبقات مملکت)، رازسهریه(جهت نگارش اسرار پادشاهان برای اشخاص سایر ملل) و راس سهریه اشاره کرد. در این بین خط ویش دبیریه خطی رمزی محسوب می‌شده است. (ابن ندیم، ۱۳۸۱: ۲۲)

عده‌ای نیز پدیدآمدن علم حروف و جفر را به ایرانیان نسبت می‌دهند و معتقدند که علم مغانه یکی از علومی بوده که تعداد محدودی از مغان، آن را می آموختند و به عدهٔ محدود دیگری تعلیم می‌دادند. (ملکان سرشت، ۱۳۸۱: ۳) بشر گذشته از استفاده از رمز در مکتوبات، در ارتباطات کلامی نیز از رمز بهره می‌جست. از این زبان‌های رمزی می‌توان به زبان زرگری، زبان لاتی، زبان مخفی یا زبان آرگو(Argo) اشاره کرد. سارقان، زندانیان، متکدیان، بدنامان و معتادان به استفاده از این زبان‌های رمزی پرداختند. (محمدی فشارکی و دیگران، ۱۳۹۰: ۱۱۰) در تعریف دقیق زبان رمزی می‌توان 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 گفت‌وگو کنند. اساس ساختن آن، همان زبانی است که مردم یک آبادی یا یک شهر با آن صحبت می‌کنند، ولی کلمات را طوری دستکاری می‌کنند که غیر از افراد آن گروه، کسی آن را نمی‌فهمد. این نوع زبان بین اصناف و پیشه‌وران و برخی اقلیت‌های ایران مانند یهودیان یا گروه‌های کوچکی مثل کولی‌ها رواج دارد.(محمودی، ۱۳۸۹: ٤۲)

مسلمانان و رمزنگاری

با توجه به شروع بعضی از سوره‌های قرآن با حروف مقطعه و رمزگونه‌بودن این حروف، از همان ابتدا مسلمانان به اهمیت رمزنگاری پی بردند و کنجکاوی و تلاش‌های زیادی برای حل این حروف رمزی انجام دادند. اما به‌طور جدی رمزنگاری از قرن دوم هجری توجه دانشمندان و کاتبان جهان اسلام را به خود جلب کرد تا جایی‌که به‌عنوان یک علم مستقل دربارهٔ آن کتاب نوشتند. اولین کتاب‌ها دربارهٔ رمزنگاری و علم تعمیه را خلیل‌بن‌احمد فراهیدی و جابربن‌حیان

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 ۲٦۰ 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 تعمیه 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. عوض‌کردن 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: ۱۱٤– ۱۱۳؛ عالم‌زاده، ۱۳۹۰: ٦٤– ٦۳)

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 دایرهٔ ابتث یا ابتثی، مقصود ترتیب حروف است به شکل ا ب ت ث ج ح و... که از معروف‌ترین دوایر حروف به‌شمار می‌رود. هم‌چنین دایرهٔ ابجد یا ابجدی یعنی ترتیب حروف به جمل: ابجد، هوز، حطی، کلمن، سعفص، قرشت، ثخذ و ضظغ که این دایره هم معروف و در نوشتن حروف تقویم و گفتن مادهٔ تاریخ معمول است. اما دوایر مشهور و معمول که علمای فن ترتیب و مبنای عمل قرار داده‌اند، سیزده دایره است: ابتث، ابجد، اهطم، اجهب، ایقغ، اجذش، ارغی، انسغ، احست، ادیل، اجهز، افسج و اعهط. (کشوری،۱۳۸٤: ٤۱) در کتاب *بدایع العلوم کنزالرموز فی علم الفنون*، تعداد دوایر بیست و هشت مورد ذکر شده است.(فانی تبریزی، ۱۳۰۰ ق: ۱۰–٦)؛ اما حروف ابجد خود به سه قسمت ابجد صغیر، وسیط و کبیر تقسیم شده است.(کشوری،۱۳۸٤: ۳٤)

ابجد صغیر

ا	ب	ج	د	ه	و	ز	ح	ط	ی
۱	۲	۳	٤	٥	٦	ساقط	۱	۲	۳
ک	ل	م	ن	س	ع	ف	ص	ق	ر
٤	۲	٥	۱	٤	ساقط	۳	٦	۲	٤
ش	ت	ث	خ	ذ	ض	ظ	غ		
٦	۱	۳	٥	ساقط	۲	٤	٦		

ابجد وسیط

ا	ب	ج	د	ه	و	ز	ح	ط	ی
۱	۲	۳	٤	٥	٦	۷	۸	۹	۱۰
ک	ل	م	ن	س	ع	ف	ص	ق	ر
۸	٦	٤	۲	ساقط	۱۰	۸	٦	٤	۸
ش	ت	ث	خ	ذ	ض	ظ	غ		
ساقط	٤	۸	ساقط	٤	۸	ساقط	٤		

ابجد کبیر

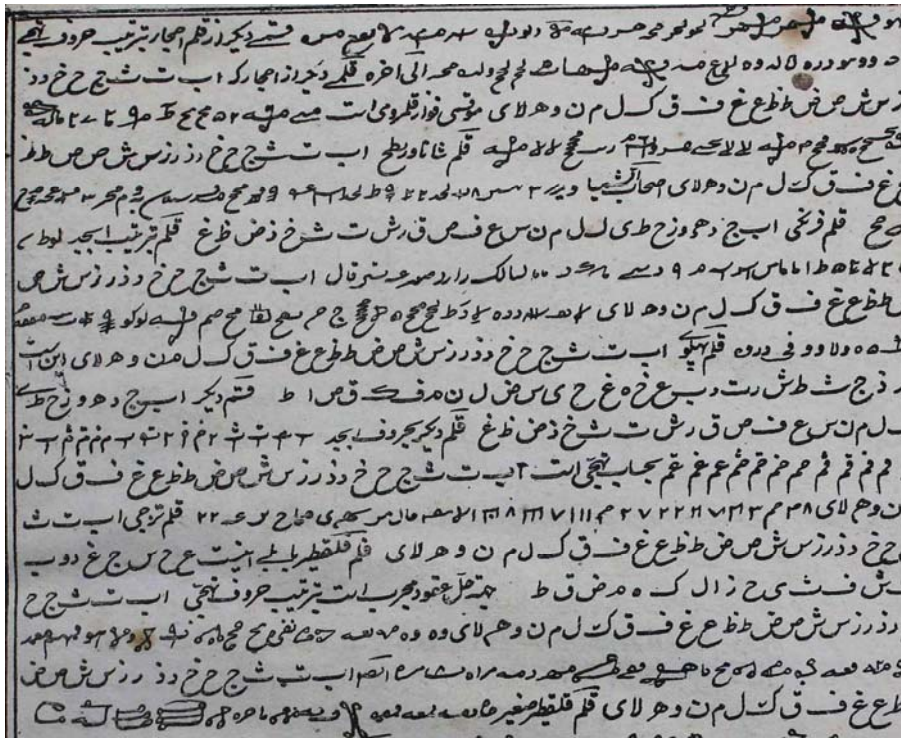
ا	ب	ج	د	ه	و	ز	ح	ط	ی
۱	۲	۳	٤	٥	٦	۷	۸	۹	۱۰
ک	ل	م	ن	س	ع	ف	ص	ق	ر
۲۰	۳۰	٤۰	٥۰	٦۰	۷۰	۸۰	۹۰	۱۰۰	۲۰۰
ش	ت	ث	خ	ذ	ض	ظ	غ		
۳۰۰	٤۰۰	٥۰۰	٦۰۰	۷۰۰	۸۰۰	۹۰۰	۱۰۰۰		

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 دربارهٔ 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

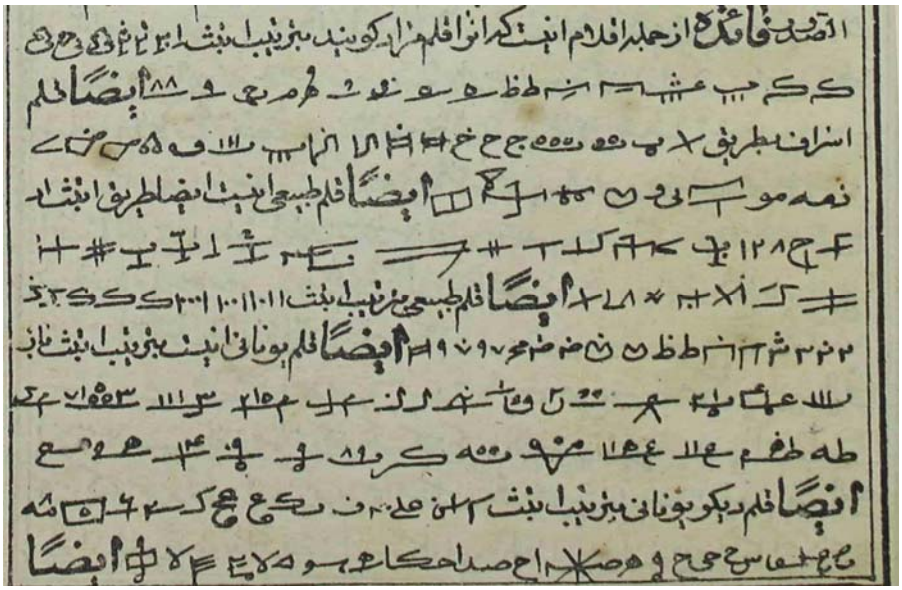
مرتضی را با یای حساب می‌کنند نه با الف و «تا»ی گرد برابرِ های گرد است. (ذاکری، ۱۳۸۸: ۱۲۳)

هر چند اطلاعات چندانی از مکاتبات رمزی در دورهٔ صفوی تا قاجار، به‌دلیل دسترسی‌نداشتن یا موجودنبودن سندی در این خصوص، نیست، اما در *خزاین* ملااحمد نراقی و به شکل کامل‌تر در *تحفه المومنین* اقلامی ذکر شده که به نظر می رسد این اقلام در مکاتبات رمزی آن دوره‌ها مورد استفاده قرار می گرفته است. در *خزاین* ملااحمد نراقی به چند نوع از اقلام رمزی اشاره شده است که از آن جمله می‌توان به قلم مراد به‌ترتیب ابتث، 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 قلیسیطین نوش حکیم، قلم سرمانوس حکیم، قلم ریحان و قلم کاشفی. (نراقی، ۱۳۰۸ق: ۲٦٥-۲٦٤) در کتاب *تحفهٔ المؤمنین* 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 به‌ترتیب ابجد لوط، قلم پهلوی، قلم قلقطیر بابلی، قلمی به حروف تهجی جهت حل عقود مجرب، قلم قلقطیر صغیر، قلم کاهی، قلم صینی، قلم جابربن‌حیان، قلم حمیمی، قلم ارمابوی، رملی مقطع، تحلیل، رومی، مشجر دیسقوردیدوس، سیمیای کبیر، سیمیای صغیر، العقول، الصابی، داودی، اسماعیلی، جعفری، الاسرار، قلم حمیری، مشجر یا سروک و چند نمونهٔ دیگر از خطوط رمزی دیگر به‌صورت تهجی ذکر کرده و نمونهٔ اقلام مذکور را نیز آورده است.(حکیم مومن، ۱۲۹۰ ق: 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 به‌درستی 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 به‌دلیل شباهتش به درخت، به خط یا قلم شجری معروف شده است. خط عمودی و خطوط مایلِ شاخه‌گونه در طرفین، نشانهٔ حروف آن است. هر حرف شجری یا هر درخت از نظم خاصی پیروی می‌کند؛ شاخهٔ سمت راست، غیر از حروف کلمهٔ ابجد، نشانهٔ کلمه و شاخهٔ سمت چپ نشانهٔ حرف است. در حروف ابجد هیچ شاخه‌ای در طرف راست نیست و این نشانهٔ کلمه ابجد است و به‌ترتیب از حرف اول تا چهارم از یک تا چهار شاخه در طرف چپ قرار دارد. در حروف هوز یک شاخه در طرف راست نشانهٔ کلمهٔ هوز و شاخه‌های طرف چپ نشانهٔ «هـ و ز» است و به‌همین‌ترتیب تا آخرین حرف این نظم برقرار است.(کسایی، ۱۳۸۷: ۱۹۷-۱۹۵)



نمونه‌ای از اقلام رمزی ذکر شده در نسخهٔ *تحفهٔ المومنین*



نمونه‌ای از اقلام رمزی ذکرشده در نسخهٔ *خزاین*

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 حوزهٔ رمزنگاری آغاز کردند و ماشین‌های رمز پیشرفته‌ای را تولید و عرضه کردند. ازجمله معروف‌ترین این ماشین‌های رمز، ماشین رمز انیگما بود که فردی آلمانی به نام آرتور شربیوس آن را در سال ۱۹۱۸م طراحی کرد و ساخت. این ماشین در آن زمان آن‌قدر 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 به‌سرعت در صنعت رمز ظهور پیدا کرد، رمزکننده‌های دیجیتال ساخته شد که در ارتباطات امن به کار گرفته شدند.

ایرانیان نیز تا پیش از دورهٔ قاجار و حتی اوایل این دوره، نیاز چندانی جهت اختراع شیوه‌های جدید برای رمزنگاری احساس نمی‌کردند. اما هر شیوهٔ 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) به‌طورکلی ضعف و کارآیی‌نداشتن رمزنگاری سنتی را می‌توان در گزینه‌های زیر خلاصه کرد:

۱. سادگی، تکراری‌بودن اقلام و شیوه‌های پیشین و نداشتن تلاش رمزشناسان آن حوزه به منظور روزآمدکردن 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 به‌ترتیب پربسامد هستند: «المونتری»، «عهدک»، «صبح قفس»، «زجش»، «خطظ»، «تضذغ» یا در زبان فارسی ترکیب حروف «اردیمون»، «هبتلشسک»، «خزع»، «قحفگ»، «جطص/پچض»، «ذغظژث» به ترتیب پربسامدترین حروف به شمار می‌آیند.(مفتاح‌الملک، ۱۳۲۰ ق: ٤۲ و ٦۳) رمزشناسان در رمزگشایی از روش‌های رمزنگاری با استفاده از حروف ابجد و سایر دوایر حروف نی، کار سختی پیش رو نداشتند؛ چرا که با برابر هم قراردادن حروف و اعداد مربوط به هر کدام به‌راحتی می‌توانستند رمز را کشف کنند؛

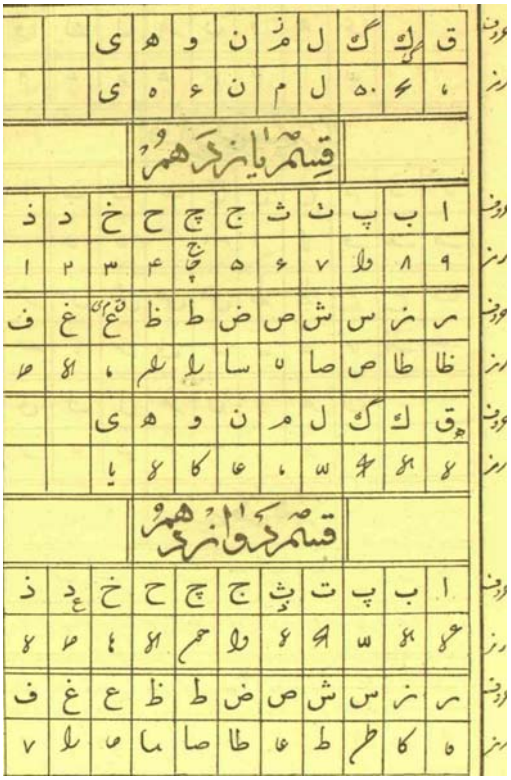
۲. دشواری استفاده از این‌گونه اقلام رمزی در ارسال پیام‌های تلگرافی؛ چرا که در بسیاری از این رموز از نشانه‌ها و اشکال مختلف استفاده شده بود؛

۳. برجسته‌شدن جنبهٔ تفننی رمزنگاری سنتی و در نتیجه عمومی‌شدن و گسترش فراگیری فنون آن.

اقلام رمزی قائم مقام فراهانی

در این دوره علاوه‌بر استفاده از اقلام رمزیِ 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 دورهٔ قاجار مشاهده کرد.(ساکما، ۲۹۵/۷٤۲۵) از ویژگی‌های عمدهٔ 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 بسنده‌نکردن 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 شایستهٔ توجه است.

مفتاح‌الملک در این خصوص به تشریح «خطوط مرموزه» جدید قبل از ایجاد تلگراف(در سدهٔ سیزدهم) می‌پردازد که خود او و به دستور ناصرالدین‌شاه کشف کرده است. «نوشتجات مرموزهٔ بسیار از زمان خاقان جنت مکان فتحعلی‌شاه 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 عدیدهٔ 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 کتابخانهٔ مبارکهٔ دولتی مضبوط بود.» (مفتاح‌الملک، ۱۳۲۰ق: ۲۲) وی اقسام خطوط اختراعیِ قائم مقام و مفاتیح آنها را پانزده مورد ذکر کرده است.(همان: ۳۱-۲٤)



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

رمز یوسفی

تشکیل وزارت امورخارجه در دورهٔ قاجار و آشنایی سفرای اعزامی به خارج با وضع و ترتیب رمزنویسی در سایر کشورها و لزوم ارسال «نوشتجات مخفیه» برای مأموران اعزامی به خارج از کشور، عده‌ای را به فکر ترجمه و تألیف کتاب‌هایی در این زمینه انداخت.(بران مرتنس، ۱۳۹٤: ۷٦-۷٤) در ایران اولین کسی‌که اقدام به تألیف اثرِ رمزی مناسب به منظور ارسال تلگراف‌های رمز کرد، میرزایوسف‌خان مستشارالدوله بود. به‌همین 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 قنسولگری 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 مرموزهٔ 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 پیداکردن دیگران می‌توانند مابین خود قرار بدهند.»(مستشارالدوله، بی‌تا: ۲) وی در توضیح مفتاح با این رمز به قاعده جمع می‌نویسد: «طرز اول به قاعدهٔ جمع است یعنی زایدکردن عددی که مابین دو شخص از سابق قرار داده شده» است، بدین‌ترتیب که دو فرد متعاهد برای ارتباط رمزی با یکدیگر، ابتدا عددی را انتخاب و معهود قرار داده و به اعداد رمزشده، اضافه کرده و پیام را ارسال می‌کنند. به‌عنوان نمونه اگر مفتاح دو شخص متعاهد عدد ۲۱٤ باشد و قرار آنها عمل جمع باشد، باید این عدد را زیر اعداد رمزشده(استخراج از کتاب *رمز یوسفی*) نوشته و آن را به اعداد مزبور اضافه کرده، حاصل جمع را به دست آورده، پس از اضافه‌کردن این عدد به اعداد رمز و ارسال آن، طرف مقابل از هر کدام از اعداد رمز به طور جداگانه۲۱٤ را کم کرده و ارقام اصلی رمز به دست می‌آید. مثلاً برای ارسال جملهٔ « ایلچی امریکا وارد تهران شدند» ابتدا با استفاده از *رمز یوسفی* اعداد معادل هر کدام از کلمات را به‌این‌ترتیب زیر آن نوشته:

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

بعد از آن عدد ۲۱٤ را به هر کدام از اعداد بالا اضافه کرده که به‌ترتیب اعداد۸۹۳۳–۵۷۳۱، ٦۱۵۱، ۹۲۰۹، ۱٤۵۱، ۲۱۳۲ به دست می‌آید، این اعداد به‌عنوان پیغام رمز ارسال می‌شود و دریافت‌کننده باید عدد۲۱٤ 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 قاعدهٔ تفریق یعنی کم‌کردن عدد معین و معهود از اعداد رمز شده است. در این روش اگر همان مثال قبلی را در نظر بگیریم، عدد ۲۱٤ را از اعداد رمز کم کرده و بعد از ارسال، طرف مقابل عدد مفتاح یعنی ۲۱٤ 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 قاعدهٔ 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،

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

رمز محمودی

محمودبن‌یوسف مازندرانی ملقب به مفتاح‌الملک، از معروف‌ترین رمزنویسان دورهٔ قاجار به‌شمار می‌رود. وی برای رمزگشایی بسیاری از رموز «قدیمه» به دریافت لقب و منصب «منشی رموزی و کفالت مطالب و مخابرات محرمانه و مرموزهٔ دولتیه» در سال ۱۲۸٦ ق. سرفراز شد.(همان: ۳) او دربارهٔ کار خود می‌نویسد: «هر قدر و از هرجا خطوط مرموزهٔ قدیمه و جدیده به دست آمده است، بدون هیچ سابقه و اطلاع از وضع واضع آنها منکشف ساخته و خود نیز انواع رمزها اختراع و وضع کرده و کتاب‌ها در معرفت آنها ترتیب داده که سال‌هاست مخابرات محرمانه و مرموزهٔ دولتیه از روی آنها معمول و دایر است.»(همان: ۵) مفتاح‌الملک در کتاب‌های خود انتقادات زیادی را بر شیوهٔ 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 اقلام مرموزه» مثل آن می‌داند که «کسی برای حفظ خانهٔ 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 حرکت‌دادن سنگ‌ها با نردبان با کمال سهولت از بام داخل خانه شده و آنچه بخواهد ببرد.»(همان: ٦و ۲۱)

وی بهره‌بردن از اقلام رمزی قدیمی به منظور ارسال تلگراف به «ممالک خارجی» را مناسب نمی‌داند و می‌نویسد: «هرگاه در ازمنهٔ سالفه مطالب محرمانه را با اقلام غریبه و سایر رمزها نوشتند چون آنها در نوشتجات سربسته و ممهور 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 مخابره می‌نمایند و صورت آنها در تمام تلگرافخانهای[تلگرافخانه‌های] داخله و خارجه ثبت و ضبط می‌شود و معایب بی‌استحکامی آنها و نتایج وخیمهٔ مترتبه بر آن ظاهر و عیان و مستغنی از شرح و بیان است.»(همان: ٦)

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

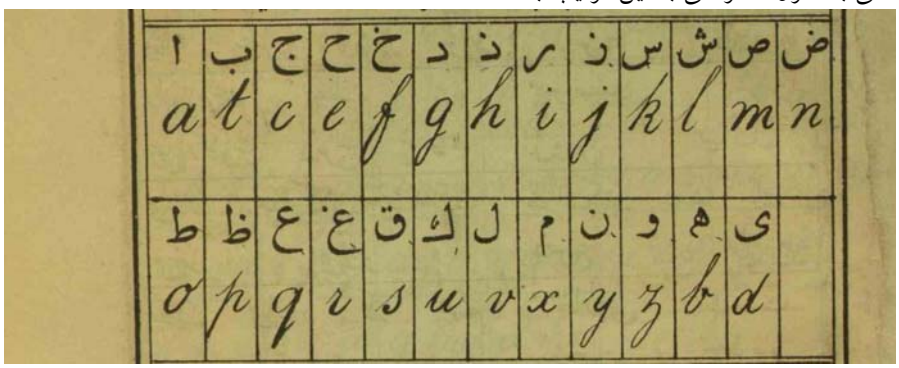
«قسم اول آن است که هر دو نفر برای مخابرات محرمانه مابین خود الفبایی ترتیب داده در مقابل هر حرفی از حروف تهجی یک رقم یا دو رقم از ارقام هندسیه رسم کرده و معهود قرار می‌دهند که در وقت ضرورت مطالب محرمانهٔ خود را از روی آن مخابره و تلگراف نمایند. قسم دیگر آن است که الفبایی نوشته و در مقابل هر حرفی از آن حرفی دیگر از حروف تهجی یا حروف جمل گذاشته و در وقت ضرورت به‌جای حروف مطلب مقابل آنها را می‌نویسند. قسم دیگر آن است که بعضی از حروف تهجی را تبدیل کرده و بعضی دیگر را به حالت خود می‌گذارند. قسم دیگر آن است که الفبایی به ترتیب ابتثی و یا به ترتیب ابجدی و یا هر ترتیب دیگر که بخواهند می‌نویسند و قرار می‌دهند که در وقت نوشتن رمز حروفی که لازم شود در آن الفبا پیدا کرده و حرف ماقبل آن و یا حرف مابعد آن را که معهود قرار داده‌اند، در عوض آن می‌نگارند. و قسم دیگر رمز یوسفی است.» مفتاح‌الملک 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 هیچ‌کدام از خطوط رمز را شایسته برای «مخابرات مرموزهٔ دولتیه» 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 مرکبهٔ کثیر الاستعمال از اسامی، افعال و ضمایر و کلمات و اصطلاحات خارجی» که در نوشتجات و مخابرات تلگرافی لازم می‌شد، به‌ترتیب حروف تهجی به‌صورت ثلاثی(سه حرفی)آورده شده است. حروف استفاده‌شدهٔ 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)

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

برای رمزکردن مطلبی با استفاده از حروف تهجی و با توجه به کتاب *ناسخ الرموز*، ابتدا میان دو طرف کلید رمزی ترتیب داده می‌شد، به‌این‌ترتیب که به جای هر یک از بیست و پنج حرف انتخاب شده، حرف دیگری قرار داده و طرفین، نسخه‌ای از آن را نزد خود نگاه می‌داشتند و هنگام مخابرهٔ تلگراف، حروفی را که در کتاب رمز، مقابل کلمات نوشته بودند، به حروف کلید تبدیل می‌کردند. برای استخراج پیام رمزشده، طرف مقابل از روی کلید مزبور که نسخه‌ای از آن را در اختیار داشت، این حروف را به حروف اصلی برمی‌گرداند و از روی لغت

ناسخ الرموز، مطلب را استخراج می‌کرد.(همان: ۱۵-۱٤؛ ساکما، ۲٤۰/۳۹۷۱۷) 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: ۱٦) مثلاً اگر بین دو نفر کلید تبدیل حروف رمز ثلاثی به حروف فرنگی به این ترتیب باشد:

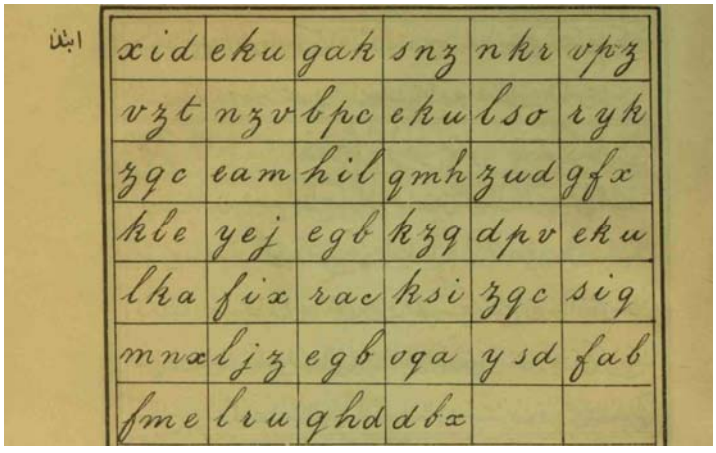


و بخواهند مطلب زیر را به رمز بنویسند:

«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 *ناسخ الرموز* 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 *ناسخ الرموز* پیدا کرده و حروف برابر هر کدام را در زیر آن نوشت.

واقعاً	لازم بود	و	خیلی مفصل	مطلب	تلگراف رمز شما رسید
و ظ ل	غ س ض	و ض ق	س ا د	ک س ح	ی م ر
را	عمده	مطلب	این	می‌خواستید	اگر
س ن غ	ط ق ش	ک س ح	ج ظ ه	ل و ض	ب و ل
می‌شد	مبلغی گزاف اجرت تلگراف	تلگراف کنید	رمزها	سایر	با
م خ د	ی ک و	د ض ع	ش ر ذ	ص ا ح	ج ع و
مطلب	می‌افتاد	که	هم	خارجی	بدست
ک س ح	ل ظ ی	ع و س	ه د ح	ز ح ن	ح ش س
کتاب	با	حالا که	اما	می‌فهمید	آن را
ع ر ق	ج ع و	ر ق س	ج ا غ	م ر خ	ا س ش
و هم	خیلی کم شده است	اجرت تلگراف	هم	نوشته‌اید	ناسخ‌الرموز
ه ا خ	ی ق ن	ا ع ط	ه د ح	و ز ش	م ض ص
		نخواهد شد	احدی از این مطلب مطلع	مفتاح	بدون
		م ه ی	ی ذ ع	ک غ ش	ح ص خ

سپس با استفاده از کلید ذکر شده حروف را به لاتین تبدیل کرده و بـه ترتیـب ذیـل بـرای طرف مقابل ارسال کرد.(همان:۹)


ابتدا

xid	eku	gak	snz	nkr	vpz
vzt	nzv	bpc	eku	lso	ryk
zqc	eam	hil	qmh	zud	qfx
kle	yej	egb	kzq	dpv	eku
lka	fix	rac	ksi	zqc	sig
mnx	ljz	egb	oqa	ysd	fab
fme	lru	qhd	dbx		

مفتاح‌الملک در همین نسخهٔ *ناسخ الرموز* 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 کلمهٔ 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 ۱۳۱٤ ق.، 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 صرفهٔ مجدد مغتنم دانسته قرار مخابرات مرموزهٔ خودمان را با ممالک خارجه به این‌طور دادیم که در وقت مخابرهٔ تلگرافی هر سه کلمهٔ رمز خودمان را که عبارت از نه حرف است متصل و بلافاصله بنویسیم که در این‌صورت در تلگراف‌خانه‌های خارجه این سه کلمهٔ رمز ما را که نه حرف است دو کلمه محسوب دارند، پس از این بابت هم یک ثلث علاوه‌بر صرفهٔ سابق صرفهٔ مجدد برای ما حاصل شده است.»(همان: ۲٤۷)

پیش از این و در سال ۱۳۱۳ ق. مفتاح الملک «چون در مخابرهٔ مطالب مرموزهٔ تلگرافی با ممالک خارجه و ولایات داخله، در تلگراف‌خانه‌های داخله و خارجه بلکه از طرف اغلب نویسندگان رمزها هم به‌طوری‌که لازم است، اهتمام و دقت کامل نمی‌شود و مقابله و تصحیح صحیح چنان که باید به عمل نمی‌آید، لهذا غالباً مطالب مرموزهٔ تلگرافی مغلوط می‌شود»، اقدام به نوشتن کتاب *کشف الاسرار ناصری* با هدف رفع این «اشکالات و محظورات» کرد.(مفتاح الملک،۱۳۱۳ق: ٤-۳) در این کتاب علاوه‌بر سه باب کتاب *ناسخ الرموز*، دو باب دیگر هم به ترتیبی خاص افزوده که وضع و ترتیب فصول آن همانند وضع و ترتیب فصول باب دوم و سوم کتاب *ناسخ الرموز* 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:۵-٤)

Aboutaleb	ابوطالب	شهر جمادی الثانیة
Oporto	اپورت	شهر رجب المرجب
Atabe	اتابك	شهر شعبان المعظم
Etalle	اتال	شهر رمضان المبارك
Atane	اتان	شهر شوال المكرم
Atrek	اترك	شهر ذیقعدة الحرام
Autriche	اتریش	شهر ذیحجة الحرام

فصل دوم در ماههای رومی

Attique	اتیك	تشرین اول
Ahmed	احمد	تشرین آخر
Akhal	اخال	كانون اول

Cintra	سنترا	از سفارت دولتین باطهار کرده
Sindjab	سنجاب	از سفارت کبرای دولت
Singueledj	سنگلج	از نقبای اقدامات خودتان اطلاع بدهید
Sinandedj	سنندج	اسباب اغتشاش رحمت شده است
Suez	سوئز	اسفراج تلگراف فرمانفرما باجناب عالی برسید
Souti	سوتی	اقدامات شما در خاکپای مبارك اشرف پادشاه افتاد
Soudan	سودان	اقدامات لازمه بعمل آمده است
Suffolk	سوفالك	اقدامات لازمه بعمل بیاورید
Suhla	سوهلا	اگر این کار را تمام کردید
Suisse	سویس	امر به مقرر فرمودند
Sohrab	سهراب	اولیای دولت علیه
Siam	سیام	اینجانب مذاکرات لازمه خواهند شد

در سال ۱۳۰۲ شمسی، مفتاح الدوله پسر مفتاح‌الملک، *ناسخ الرموز* را تجدید چاپ کرد و در آن از جزوهٔ مهدی صلحی، ناظم الحکما، نیز استفاده کرد که شامل لغاتی جدید بود و در تبریز در سال ۱۳۰۰ش. چاپ شده بود. در سال ۱۳۱۰ش. وزارت جنگ در نامه‌ای به ریاست وزرا، *ناسخ الرموز* را برای «مخابرات رمزی آن وزارتخانه» به دلایل محدودنبودن مطالب رمزی قشونی، اتلاف وقت و نداشتن جملات و کلمات ضروری و لغات لازم در مخابرهٔ 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 دربارهٔ اختصاص طبع و فروش *ناسخ الرموز* 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 *ناسخ الرموز* 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، ۲٤۰/۷۵٦٤۷؛ ۲۹۳/۵٤۹۲۳) 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 تعمیه 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 دورهٔ 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 آسان‌بودن رمزگشایی از این اقلام و نیز مشکلاتی نظیر ترکیب حروف و ارقام و اشکال، به‌خصوص در مخابرهٔ پیام‌های تلگرافی امر دشواری بود. بنابراین

عده‌ای در صدد برآمدند تا با توجه بـه رمزنگـاری اروپاییـان در مکاتبـات محرمانـهٔ تلگرافـی، کتاب‌هایی را در این زمینه به نگارش درآورند که از مهم‌ترین این کتاب‌ها، می‌تـوان بـه کتـاب *رمز یوسفی* نوشته یوسف‌خان مستشارالدوله اشاره کرد. این کتاب مبتنی‌بـر رمزنگـاری عـددی بود که تا چندی در مکاتبات رمزی تلگرافی استفاده شد. اما بار اصلی در این راه را محمودخان مفتاح‌الملک از رجال دورهٔ ناصری بر دوش کشید. مفتاح‌الملک با نوشتن کتاب *ناسخ الرموز* که رمزی حروفی بود، مدتی طولانی یکه‌تاز میدان رمزنگـاری در دورهٔ قاجـار و پهلـوی شـد، بـه طوری‌که این کتاب بعد از چند بار تجدیدنظر و چاپ، مهم‌ترین مرجع وزارتخانه‌هـای دولتـی در زمینهٔ ارسال پیغام‌های رمزی به حساب می‌آمد و از اعتبار شایان‌توجهی برخوردار بود. رمـز مزبور که به رمز محمودی نیز مشهور است، به صورت ثلاثی بوده و علاوه‌بر سادگی استفاده از آن، بعد از انتخاب کلید مدنظر، از لحاظ مالی نیز برای ارسال‌کننـدگان بـسیار بـه صـرفه بـود. بنابراین مفتاح‌الملک با آگاهی از ضعف سایر اقلام رمزی و به‌خصوص در ارسال تلگراف‌هـای محرمانه به خارج از کشور، موفق به اختراع رمزی شد که جهت ارسال ایـن‌گونـه پیغـام‌هـا در داخل و خارج از کشور، اعتبار بسیاری داشت و رمزگشایی آن بدون کلید کـار دشـواری بـود، بنابراین اعتبار آن موجب دوام استفاده از آن در دستگاه‌های دولتی و مأموران سیاسی ایـران در خارج و ایجاد کانالی امن در ارتباطات رمزی شد.

کتاب‌شناخت

اسناد

سازمان اسناد و کتابخانهٔ ملـی ایـران(سـاکما)، اسـناد شـمارهٔ ۳۱۰/۳۱۰۹۸، ۲٤۰/۳۹۷۱۷، ۲٤۰/۷۵٦٤۷، ۲۹۵/۷٤۲۵، ۲۹۳/۷۳۲۰، ۲۹/۵٤۹۲۳.

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

نسخ چاپ سنگی

فانی تبریزی، اسماعیل‌بن‌محمدصادق (۱۳۰۰ ق) *بدایع‌العلوم کنزالرموز فی علم‌الفنون*، سـازمان اسـناد و کتابخانهٔ ملی ایران، شمارهٔ دستیابی ۹٦۸٦ـ٦.

مازندرانی، محمودبن‌یوسف(مفتاح الملک) (۱۳۱۳ ق) *کشف الاسرار*، سـازمان اسـناد و کتابخانـهٔ ملـی، شمارهٔ دستیابی ۱٦۳٦۹-٦.

_____(۱۳۱۹ ق) *ناسخ الرموز و رمز محمودی*، سازمان اسناد و کتابخانهٔ ملی، شمارهٔ دستیابی ۲۳۱۲۷-٦.

_____ (۱۳۲۰قمری) *مفتاح الرموز*، چاپ سـنگی، سـازمان اسـناد و کتابخانـه ملـی، شمارهٔ دستیابی ۱٤۰٦۹-٦.

محمدمؤمن‌بن‌محمدزمان(حکیم مومن) (۱۲۹۰ق) *تحفهٔ المومنین*، سازمان اسناد و کتابخانهٔ ملی، شـمارهٔ دستیابی، ۱۸۸۰۱-٦.

مستشارالدوله، یوسف‌بن‌کاظم (بی‌تا) *رمز یوسفی*، چاپ سنگی، سازمان اسناد و کتابخانهٔ ملی، شمارهٔ دستیابی ۵۰۳۳-٦.
نراقی، ملااحمد (۱۳۰۸ ق) *خزائن*، چاپ سنگی، سازمان اسناد و کتابخانهٔ ملی، شمارهٔ دستیابی ٦-۲٦٤۳٦.

کتاب‌ها

ابن ندیم، محمدبن‌اسحاق (۱۳۸۱) *الفهرست*، مترجم و محقق: محمدرضا تجدد، تهران: اساطیر.
اسماعیل‌پور، جمشید (۱۳۸۹) *آلبوم خط و نشانه‌های باستان*، تبریز: احرار.
شیخ‌زادگان، جواد (۱۳۸۹) *رمزشناسی مقدماتی*، تهران: پژوهشکدهٔ پردازش هوشمند علائم.
شیری، مینا (۱۳۹۳) مقدمه‌ای بر رمزنگاری: از رمزنگاری کلاسیک تا رمزنگاری کوانتومی، تهران: دانشیاران ایران.
صفری ممقانی، عیسی(۱۳۹٦) *حروف رمزی در فرهنگ و تمدن ایران*، تهران: پازینه.
کشوری، ارسلان (۱۳۸٤) *کله‌سر*، چاپ۲، تهران: جهان‌تاب.
محمودی، نرگس (۱۳۸۹) *رمزنویسی و گویش‌های رمزی*، تهران: خیام آزمون، علوم پارسی.
مرتنس، بران (۱۳۹٤) *قوانین السفرا(رساله‌ای در باب آداب دیپلماسی زمانهٔ 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»، آینهٔ میراث، شمارهٔ ٤۵، پاییزو زمستان.
عالم‌زاده، هادی(۱۳۹۰)، «رمزنگاری در نامه‌ها» در صبح الأعشی فی صناعة الإنشاء، ابوالعباس احمدبن‌علی قلقشندی ٦۵۷-۸۲۱ق)، نامهٔ بهارستان، سال ۱۲، شمارهٔ ۱۸ و ۱۹، بهار و تابستان
کسایی، سیدعلی(۱۳۸۷) «خط شجری»، آینهٔ میراث، شمارهٔ ٤۲، پاییز
محمدی فشارکی، محسن و مریم شیرانی (۱۳۹۰) «خط معما؛ پژوهش در انواع و شیوه‌های رمزنگاری منشآت»، متن‌شناسی ادب فارسی، شمارهٔ۱۱، 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, Esmāīl 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), *Kašf 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), *Nāsiḵ al-Romūz va Raz-e Maḥmūdī*, SAKMA, 23127-6.
- Moḥammad Momin b. Moḥammd b. Moḥammad Zamān (Ḥakīm Momin) (1290), *Toḥfat al-Mominīn*, SAKMA, 18801-6.
- Mostašār al-Dolla, Yūsif b. Kāẓim, *Ramz-e Yūsifī*, Litographed, SAKMA, 5033-6.
- Narāqī, Mollā Aḥmad (1308), *ḵazāīn*, Litografed, SAKMA, 6-26436.

Books
- Esmāīlpūr, ĵamšīd (1389 Š.), *Ālbum-e ḵaṭ va Nišānahā-ye Bāstān*, Tabriz: Aḥrār. [In Persian]
- Ibn Nadīm, Moḥammad b. Esḥāq (1381 Š.), *Al-Fihrist*, Translated and edited by Moḥammad Reżā Taĵaddod, Tehran: Asāṭīr. [In Persian]
- Kišvarī, Arsalān (1384 Š.), *Kala Sar*, Tehran: ĵahāntāb. [In Persian]
- Maḥmūdī, Nargis (1389 Š.), *Ramznivisī va Gūyišhā-ye Ramzī*, Tehran: ḵayyām Āzlūn, ‘Olūm-e Pārsī. [In Persian]
- Malikān Sirišt, Moḥammad (1381 Š.), *Ṭāli‘bīnī-e Āryāīī*, Tehran: Naḏīr. [In Persian]
- Ṣafarī Mamqānī, ‘Īsā (1396 Š.), *Ḥorūf-e Ramzī ddar Farhang*, va Tamaddon-e Īrān, Tehran: Pāzīna. [In Persian]
- Šaiḵzādigān, ĵavād (1389 Š.), *Ramzšināsī-ye Moqadamātī*, Tehran: Peĵūhiškada-ye Pardāziš-e Hūšmand-e Alāim. [In Persian]
- Šīrī, Mīnā (1393 Š.), *Moqadamaīī bar Ramznigārī: Az Ramznigārī-ye Klasīk tā Ramznigāri-ye Koāntomī*, Tehran: Dānišyārān-e Īrān. [In Persian]

Articles
- Ālimzāda, Hādī (1390 Š.), “Ramznigārī dar Nāmahā”, dar Ṣobh al-‘Ašā fi Ṣinā‘a al-Enšā Abul Abbās Aḥmad b. ‘Ali Qilqašandī 821-657 AH., *Nāma-ye Bahāristān*, 12, No. 18 & 19, Spring and Summer. [In Persian]
- Ḏākirī, Moṣṭafā (1388 Š.), “Ebdā‘-e ḵoṭūṭ-e Ramzī dar Farhang-e Eslāmī va Īrānī”, *Āīīna Mīrāṯ*, No. 45, Fall & Winter. [In Persian]
- Kasāīī, Sayyed ‘Alī (1387 Š.), “ḵaṭ-e Šaĵarī”, *Āīīna-ye Mīrāṯ*, No. 42, Fall. [In Persian]
- Mirtins, Brān (1394 Š.), *Qavānīn al-Sofarā (Risāla dar Bāb-e Ādab-e Dīplomāsī-ye Zamāna-ye Qāĵār*, translated by Mīrzā Ebrāhīm Malkom, Edited by Ṣobḥ ḵosravīzāda & Fāṭima Amīrī Parī, Tehran: Mohāĵir. [In Persian]
- Moḥammadī Fišārakī, Moḥsin; Šīrānī, Maryam (1390 Š.), “ḵaṯ Mo‘amā; Peĵūhiš dar Anvā‘ va Šīvahā-ye Ramznigārī-ye Monšaāt”, *Matnšināsī-ye Adab-e Fārsī*, No. 11, Fall. [In Persian]

Historical Perspective & Historiography, Vol.29, No.24, 2020
Alzahra University, http://hph.alzahra.ac.ir/

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