لزوم حفاظت از بعضی اطلاعات در برابر دسترسی افراد غیر مجاز، احتمالاً دغدغه بشر از آغازین روزهای اختراع خط بوده است. این دغدغه منجر به ابداع روش‌های متنوعی برای حفظ اطلاعات در برابرافراد فاقد صلاحیت در طول تاریخ شده است. به عنوان مثال اسپارت‌ها[1] ۴۰۰ قبل از میلاد مسیح روشی برای انتقال فرمان‌ها و اطلاعات نظامی ابداع کرده بودند. آنها یک نوار پارچه‌ای را به دور یک استوانه به صورت مارپیچ می‌بستند، سپس پیغام مورد نظر را روی نوار به صورت افقی می‌نوشتند. نوشتهٔ روی نوار پس از باز کردن نوار غیر قابل فهم بود چرا که حروفی که هنگام نوشتن مجاور هم بودند پس از باز کردن نوار دیگر مجاور هم نبودند. کسی قابلیت بازیابی متن را داشت که استوانه‌ای برابر استوانه نویسنده داشت و نوار را به صورت مارپیچ روی استوانه خود می‌پیچید.

ژولیوس سزار[2] (۱۰۰ تا ۴۴ ق‌م) کنسول و دیکتاتور روم برای ارسال فرمان‌های نظامی از سامانهٔ رمزی استفاده می‌کرد که امروزه به نام خود وی شـناخته می‌شود. در سامانهٔ رمز سزار برای رمز کردن متن به جای هر حرف، یک نوار پارچه‌ای را به دور یک استوانه به صورت مارپیچ می‌بستند، سپس پیغام مورد نظر را روی نوار به صورت افقی می‌نوشتند. نوشتهٔ روی نوار پس از باز کردن نوار غیر قابل فهم بود چرا که حروفی که هنگام نوشتن مجاور هم بودند پس از باز کردن نوار دیگر مجاور هم نبودند. کسی قابلیت بازیابی متن را داشت که استوانه‌ای برابر استوانه نویسنده داشت و نوار را به صورت مارپیچ روی استوانه خود می‌پیچید.نوشته می‌شود. به گفتهٔ مورخان، آگاستاس[3] (۶۳ ق‌م تا ۱۴م) امپراطور اول روم هم از سامانهٔ رمزی مشابه سامانهٔ سزار برای رمز کردن متون مهم استفاده می‌کرد. در سامانهٔ مورد استفاده آگاستاس، به جای هر حرف متن اصلی، حرف بعد در الفبای لاتین و به جای حرف Z، از AA استفاده می‌شد.

یکی از نکات برجستهٔ تاریخ رمزنگاری، اختراع روش رمزگشایی سامانه‌های رمزنگاری که مشابه یک نوار پارچه‌ای را به دور یک استوانه به صورت مارپیچ می‌بستند، سپس پیغام مورد نظر را روی نوار به صورت افقی می‌نوشتند. نوشتهٔ روی نوار پس از باز کردن نوار غیر قابل فهم بود چرا که حروفی که هنگام نوشتن مجاور هم بودند پس از باز کردن نوار دیگر مجاور هم نبودند. کسی قابلیت بازیابی متن را داشت که استوانه‌ای برابر استوانه نویسنده داشت و نوار را به صورت مارپیچ روی استوانه خود می‌پیچید. [4] معروف است در نوشتهٔ او با عنوان «رساله فی الاستخراج المعما» آمده است. اساس تجزیه و تحلیل بسامد مبتنی بر این واقعیت است که در هر نوشته‌ای از هر زبانی، حروف متفاوت و تر یک نوار پارچه‌ای را به دور یک استوانه به صورت مارپیچ می‌بستند، سپس پیغام مورد نظر را روی نوار به صورت افقی می‌نوشتند. نوشتهٔ روی نوار پس از باز کردن نوار غیر قابل فهم بود چرا که حروفی که هنگام نوشتن مجاور هم بودند پس از باز کردن نوار دیگر مجاور هم نبودند. کسی قابلیت بازیابی متن را داشت که استوانه‌ای برابر استوانه نویسنده داشت و نوار را به صورت مارپیچ روی استوانه خود می‌پیچید. یک نوار پارچه‌ای را به دور یک استوانه به صورت مارپیچ می‌بستند، سپس پیغام مورد نظر را روی نوار به صورت افقی می‌نوشتند. نوشتهٔ روی نوار پس از باز کردن نوار غیر قابل فهم بود چرا که حروفی که هنگام نوشتن مجاور هم بودند پس از باز کردن نوار دیگر مجاور هم نبودند. کسی قابلیت بازیابی متن را داشت که استوانه‌ای برابر استوانه نویسنده داشت و نوار را به صورت مارپیچ روی استوانه خود می‌پیچید. دارنود. مهمترین سامانهٔ رمزنگاری مورد استفاده در حال حاضر

با گسترش شبکه‌های ارتباطی و به ویژه شبکه‌های کامپیوتری و پیدایش اینترنت در نیمهٔ دوم قرن بیستم میلادی نیاز به راهکارها و روش‌های جدیدی برای رمزنگاری احساس می‌شد؛ چرا که به طور مثال امروزه وقتی شما به وبگاهی وصل می‌شوید که در شهری، کشوری یا قاره‌ای دیگر میزبانی می‌شود و می‌خواهید اطلاعاتی مهم مانند اطلاعات کارت بانکی خود را به آن وبگاه ارسال کنید، این امکان وجود ندارد که قبل از وصل شدن به وبگاه با مسئولان وبگاه دیدار کرده و اطلاعات مربوط به سامانهٔ رمزانه‌های دههٔ ۷۰ میلادی با ارائهٔ راهکارهایی بدیع برای حل معضل فوق عرصهٔ تازه‌ای را در رمزنگاری شروع کردند. دیفی و هلمن این عرصهٔ تازه را **رمزنگاری کلید عمومی** نامیدند. امروزه این عرصه **رمزنگاری نامتقارن** نیز نامیده می‌شود.

در طراحی سامانه‌های رمزنگاری کلید عمومی توابع یک‌طرفه نقش کلیدی دارند. به طور اجمالی، یک تابع «از به» یک‌طرفه است اگر محاسبه برای عضوی چون «از» آسان باشد ولی محاسبهٔ معکوس تابع آسان نباشد. بدین معنی که محاسبه برای عضوی چون «از» آسان نیست و زمان بسیاری می‌برد. البته این آسان بودن با آسان نبودنِ محاسبه امروزه تدقیق شده‌اند که نیازی به تفصیل در اینجا دیده نمی‌شود. راهکار دیفی و هلمن مبتنی بر استفادهٔ هوشمندانه از توابع یک‌طرفهٔ مربوط به گروه‌های متناهی بود.

امروزه سامانه‌های کلید عمومی و توابع یک‌طرفه کاربردهای بسیاری پیدا

1. Spartans
2. Julius Caesar
3. Augustus
4. Frequency Analysis
5. Enigma
6. Lorenz

کرده‌اند که این کاربردها با استفاده از سامانه‌های کلید خصوصی یا ناممکن و یا در صورت امکان بسیار هزینه‌بر هستند. تعدادی از این کاربردها عبارت‌اند از: به اشتراک‌گذاری کلید با استفاده از یک کانال ناامن، امضای دیجیتال بدون استفاده از کلید مشترک، محاسبات چندجانبه.

مطالب فوق با فرض اینکه خواننده یک فهم اجمالی از مفهوم رمزنگاری دارد نوشته شده‌اند. مانند هر شاخهٔ علمی دیگری محققان رمزنگاری سعی کرده‌اند تعریف دقیق‌تری از رمزنگاری ارائه دهند. اگر بنا بر تعریف رمزنگاری باشد می‌توان گفت که امروزه به مجموعه روش‌ها، فرایندها، الگوریتم‌ها و پروتکل‌هایی که برای نگهداری و انتقال امن اطلاعات در حضور افراد فاقد صلاحیت استفاده می‌شوند رمزنگاری گفته می‌شود. به بیان دقیق‌تر، رمزنگاری علمی است که ارائه‌دهندهٔ چهار خدمت اصلی زیر به کاربران اطلاعات است: حفظ محرمانگی اطلاعات، حفظ تمامیت و یکپارچگی اطلاعات، احراز هویت منبع اطلاعات و در نهایت پیشگیری از عدم پذیرش تعهدات و یا اقدام‌های گذشته. دو مورد آخر نیاز به توضیح بیشتری ندارند. اما حفظ محرمانگی اطلاعات عبارت است از حفظ اطلاعات از دسترسی افراد غیرمجاز و حفظ تمامیت اطلاعات به معنای حصول اطمینان از عدم تغییر اطلاعات است. برای ارائهٔ هر کدام از این خدمات چهارگانه رمزنگاران ابزار و پروتکل‌های متنوعی طراحی کرده‌اند.

در سال‌های اخیر، تحول بسیار مهمی در رمزنگاری رخ داده است که موضوع بخش بعدی این نوشته است و سعی شده است که با تفصیل بیشتری این تحول مهم شرح داده شود.

۲. رمزنگاری پساکوانتومی

امنیت مهم‌ترین سامانه‌های رمزنگاری کلید عمومی مورد استفادهٔ کنونی مبتنی بر سختی تجزیهٔ اعداد صحیح یا سختی حل مسئلهٔ لگاریتم گسسته در گروه خم بیضوی تعریف شده روی یک میدان متناهی است. منظور از سختی به این معناست که هم اکنون اگر عدد صحیح یا خم بیضوی مورد استفاده با دقت انتخاب شوند حل مسائل مربوط حتی با استفاده از بهترین الگوریتم‌ها وداشتن امکانات محاسباتی بسیار زیاد به زمان بسیاری، به طور مثال چند ده سال، نیاز دارد. به معنای دیگر، هم اکنون الگوریتم‌های مناسبی وجود ندارند که با استفاده از آنها و کامپیوترهای امروزی بتوان مسائل فوق را در مدت زمان مناسب حل کرد. این در حالی است که در صورت ساخته شدن کامپیوترهای کوانتومی، می‌توان با استفاده از الگوریتم پیتر شر[1] مسائل فوق را در زمان کوتاهی حل کرده و سیستم‌های رمز مربوطه را شکست. لزوم حفاظت از برخی اطلاعات برای چند دهه، طراحی سیستم‌های رمزنگاری جدید که در برابر کامپیوترهای کوانتومی مقاوم باشند ضروری می‌نماید. با توجه به این ضرورت شاخه‌ای جدید در رمزنگاری در دو دههٔ گذشته پدید آمده است که به آن رمزنگاری پساکوانتومی می‌گویند. در بخش بعد به بررسی مختصر مهم‌ترین سامانه‌های رمزنگاری پساکوانتومی می‌پردازیم.

1. Peter Shor