بسم الله الرحمن الرحیم

الگوریتم رمز ورنام

در [رمزنگاری](https://fa.wikipedia.org/wiki/%D8%B1%D9%85%D8%B2%D9%86%DA%AF%D8%A7%D8%B1%DB%8C)، پد یک بار مصرف یک روش رمزگذاری است که نمی‌تواند شکسته‎‌شود ولی نیاز به کلیدی دارد که از قبل به اشتراک گذاشته شده است و طولی برابر یا بیشتر از پیام ارسالی دارد. در این روش، متن اصلی، با یک کلید مخفی رندوم، که به آن پد یکبار مصرف هم میگویند، جفت می‌شود. سپس هر بیت یا کاراکتر از متن اصلی، با ترکیب شدن با بیت یا کاراکتر معادل خود در کلید، با استفاده از جمع پیمانه‌ای، رمزگذاری می‌شود.[

اگر کلید

1. واقعا [رندوم](https://fa.wikipedia.org/wiki/%D8%B1%D9%86%D8%AF%D9%88%D9%85) باشد،

2. حداقل طولی برابر با طول متن اصلی داشته باشد،

3. هیچ وقت در کل یا در بخشی، دوباره استفاده نشود،

4. و کاملا مخفی نگه داشته شود، متن رمز شده،

قابل رمزگشایی یا شکسته شدن نخواهد بود. همچنین اثبات شده است که هر متن رمز شده با ویژگی پنهانی بودن کامل، باید از کلیدهایی با ویژگی‌های مشابه پد یکبار مصرف، به طور موثر استفاده کند.

ورژن‌‌های دیجیتالی از رمزهای با پد یکبار مصرف، توسط ملت‌ها برای ارتباطات [دیپلماتیک](https://fa.wikipedia.org/wiki/%D8%AF%DB%8C%D9%BE%D9%84%D9%85%D8%A7%D8%AA%DB%8C%DA%A9) و نظامی حیاتی، استفاده شده است. ولی مشکل توزیع امن کلید، آنها را برای بیشتر کاربردها، غیرعملی کرده است.

اولین بار در سال 1882 فرانک میلر، پد یکبار مصرف را توصیف کرد و سپس در سال 1917 بازنگری روی آن صورت گرفت. در 22 جولای 1919 برای گیلبرت ورنام به خاطر استفاده از عملگر xor در رمزگذاری با پد یکبار مصرف، حق انحصاری اختراعات صادر شد. سیستم او که از *رمز ورنام* او صادر شده بود، رمزی بود که از ترکیب یک پیام با یک کلید که از نوار پانچ خوانده میشد، ساخته می‌شد. در ساختار اصلی، سیستم ورنام آسیب پذیر بود، چون نوار کلید یک حلقه بود، که هربار این حلقه یک دوره کامل را طی میکرد، دوباره استفاده می‌شد. استفاده یک باره، بعدا و زمانی که [جوزف مابورن](https://fa.wikipedia.org/w/index.php?title=%D8%AC%D9%88%D8%B2%D9%81_%D9%85%D8%A7%D8%A8%D9%88%D8%B1%D9%86&action=edit&redlink=1) متوجه شد اگر نوار کلید کاملا رندوم باشد کشف رمز غیرممکن می‌شود، ایجاد شد.

بخش "پد" در پد یکبار مصرف، از پیاده‌سازی‌های اولیه می‌آید؛ زمانی که کلید روی یک تکه کاغذ، که اجازه می‌داد برگه بالایی فعلی بعد از مصرف خاموش و نابود شود، ارائه میشد. برای مخفی سازی، این پد گاهی خیلی کوچک بود، طوری که یک ذره بین قوی برای استفاده از آن لازم بود. سازمان امنیت ملی از برگه‌هایی با اندازه‌ای استفاده می‌کرد که در کف دست یا پوست گردو جا می‌شدند. برای افزایش امنیت، پدهای یکبار مصرف گاهی روی کاغذهایی که از نیتروسلولوز بسیار قابل اشتعال چاپ می‌شوند تا به راحتی پس از مصرف، سوزانده شوند.

کمی ابهام در مورد اصطلاح "رمز ورنام" وجود دارد چون بعضی منابع از "رمز ورنام" و "پد یکبار مصرف" به صورت هم‌معنی استفاده می‌کنند در حالی که بعضی دیگر به هرنوعی از رمز جریانی جمع پذیر از جمله آنهایی که برپایه یک شبه رندوم ساز پنهانی و رمز شده هستند، "رمز ورنام" می‌گویند.