مقدمه

رمز ورنام توسط vernam در آزمایشگاه AT&T ساخته شد.این رمز الهام بخش خیلی از رمز های دیگری که امروزه استفاده می شود.یکی از کاربرد این رمز ، استفاده ی آن در one time pad یا به صورت مخفف OTP می باشد،که یکی از موارد استفاده در رمز های پویا در پرداخت های بانکی استفاده می شود.

آقای ورنام که نام کامل آن گیلبرت ورنام می باشد،فارغ التحصیل رشته ی مهندسی از موسسه wordcester و مهندس آزمایش AT&T بود.

رمز گذاری و رمز گشایی

ساختار رمز ورنام بسیار ساده است. اگر فرض کنیم که متن ورودی یا متن اصلی را با X و متن رمز شده را با Y و کلید را با K نمایش بدهیم.

$X = (X_۱, X_۲ , ...,X_n)$

$K = (K_۱ , K_۲,.....,K_n)$

$Y = (Y_۱,Y_۲,.....,Y_n)$

رمز گذاری آن به از فرمولی که نوشته شده بدست می آید که هر X_i و K_i و Y_i نشانه ی یک بیت است.

$Y_i = X_i \oplus K_i$

بر اساس فرمولی که در بالا نوشته شده ، به این معناست که هر بیت متن اصلی را با بیت متناظر کلید در نظر گرفته شده XOR می کنیم،تا بیت آخر و سپس تمام بیت های Yرا بهم چسبانده و خروجی را رمز شده را دریافت می کنیم. این فرمول برای رمز گذاری آن است.

برای رمز گشایی،به دلیل این که عکس عمل XOR، خودش می باشد،برای رمز گشایی نیز از فرمول بالا استفاده کرده و فقط جای X را با Y عوض می کنیم. مانند بالا تمامی بیت های X را بهم چسبانده و Xبه این ترتیب بازیابی می شود.

یادآوری :

جدول صحت عملگر XOR

a	b	a⊕b
۰	۰	۰
۰	۱	۱
۱	۰	۱
۱	۱	۰

نکته در مورد رمز vernam

در این جا فرض شده بود که X,Y,K تعداد بیت های یکسانی دارند که عموما در رمز نگاری چنین چیزی وجود ندارد،پس اگر تعداد بیت ها یکسان نباشد، از ساز و کار های دیگری مانند padding استفاده می می کنیم و راه دیگر این می تواند باشد که اگر متن اصلی تعداد بیت هایش کم تر از کلید باشد،تا آن جا که می شود متن اصلی با کلید XORکرده و سپس Y بدست آمده را می توان به انتهای Xاضافه کرد.

روش پیاده سازی در نرم افزار cryptool

می توان به جای این که هر مقدار را بیت به بیت بدهیم،می توانیم داده هایی همچون متن ، فایل متنی را داده و رمز گذاری و رمز گشایی را با کلید مورد نظر ببینیم،چون در پیاده سازی از string decode استفاده شده که داده ورودی به بیت تبدیل می کند و در نقطه مقابل آن نیز string encodeمی باشد

که برعکس ، یعنی داده ی بیتی را متن تبدیل می کند و هر بار با تغییر کلید، رمز شده متن اصلی تغییر می کند. حتی می توانیم خروجی و ورودی های string تنظیم کنیم، که می توانید در نرم افزار ببنید و هربار متن و کلید را تغییر داده و خروجی ببنید و فقط برای اطمینان هم زمان که رمز گذاری انجام می شود،از خروجی XORبه گرفته و باکلید دوباره XOR می شود برای این که رمز گشایی انجام شود، که آیا متن اصلی را خروجی می گیریم یا خیر.

برای مثال فرض کنید که X=۱۰۰۰۱۱۱ و K=۰۰۱۱۰۱۱، حال مقدار Y را بدست بیاورید،در رمز vernam.

X = ۱۰۰۰۱۱۱ ,K = ۰۰۱۱۰۱۱ => Y=?

با استفاده از جدول صحت وبیت به بیت X را با K ، XOR می کنیم تا Y بدست آید.

Y = ۱۰۱۰۰۰۰

حال برای این که مطمئن شویم که درست عملیات را انجام داده ایم ، می توان متن Y با همان کلید K ،XOR کرد و متن X بازیابی می شود.

X` = ۱۰۰۰۱۱۱ = X

منابع

Wikipedia

ویدیو های آموزشی درس رایانش امن