



NOxCrypt v2.3.0 – مشخصات عمومی

نویسنده: NOX

1. نام

NOxCrypt v2.3.0 یک الگوریتم رمزنگاری اختصاصی است که به طور خاص برای سیستم NOX طراحی شده است. هدف آن ارائه رمزنگاری ای است که به عنوان رمزنگاری قابل تشخیص نباشد، از جمله با جعل به صورت فرمت های رسانه ای مختلف و جریان های دودویی تصادفی. همچنین این الگوریتم بر پایه سازوکار رمزنگاری عمیق (توسعه NOX) استوار است.

2. اهداف و ویژگی ها

- مخفی سازی نه تنها محتوای داده ها بلکه خود وجود آن ها.
- داده های خروجی می توانند تصاویر، صوت، ویدئو یا داده های دودویی دلخواه را تقلید کنند.
- جعل به شکل فرمت های رایج (مانند JPEG، MP3، PNG).
- استفاده انحصاری درون اکوسیستم NOX.
- کلید پویا که به صورت منحصر به فرد برای هر نشست تولید می شود.
- سازوکار رمزنگاری عمیق (توسعه NOX) به عنوان لایه اضافی برای حفظ حریم خصوصی.

3. معماری

معماری شامل مراحل زنجیره ای برای تبدیل داده ها است، شامل جایگزینی، ترکیب، و افزودن نویز کنترل شده. طرح های ریاضی خاص و جدول های داخلی محرمانه هستند و در نسخه عمومی این مشخصات افشا نمی شوند.

4. کلید و نشست‌ها

کلید رمزنگاری طول زیادی دارد و به‌صورت پویا با استفاده از پارامترهای تصادفی و پارامترهای جلسه ایجاد می‌شود. برای هر نشست، جدول‌ها و قواعد تبدیل منحصربه‌فردی ایجاد می‌گردند که مانع از استفاده مجدد از کلیدها و الگوهای رمزنگاری می‌شود.

5. پوشش‌دهی

الگوریتم قادر است جریان رمزنگاری‌شده را به شکلی تبدیل کند که با انواع مختلفی از فایل‌های رسانه‌ای یا ترافیک شبکه مطابقت داشته باشد، که شناسایی انتقال داده‌های رمزنگاری‌شده را بسیار دشوار می‌سازد.

6. امنیت

هر نشست از کلیدها و مجموعه قواعد رمزنگاری منحصربه‌فرد استفاده می‌کند. حتی در صورت رهگیری ترافیک، بدون دسترسی به کلید، رمزگشایی غیرممکن است. این الگوریتم شامل سازوکارهایی برای جلوگیری از تحلیل رمز و پنهان‌سازی ساختار داده است.

7. کاربرد

NOXCrypt می‌تواند متن، داده‌های صوتی و جریان‌های دودویی دلخواه را رمزنگاری کرده و آن‌ها را به شکلی تبدیل کند که مشکوک به نظر نرسند. این الگوریتم برای سرعت بالا و تأخیر پایین در انتقال داده بهینه‌سازی شده است.

8. نتیجه‌گیری

NOXCrypt یک سامانه رمزنگاری نسل جدید است که بر حداکثر محرمانگی و ناشناس‌ماندگی و همچنین مقاومت در برابر شناسایی و تحلیل تمرکز دارد. این مشخصات دید کلی از فناوری را ارائه می‌دهد و جزئیات داخلی الگوریتم را فاش نمی‌کند.