

تاریخچه‌ای کوتاه از مهر و موم

برای چهار قرن، یک قطره موم قرمز تضمین می‌کرد که هیچ‌کس نامه‌ای را نخوانده است. ما این را با ورود به عصر دیجیتال از دست دادیم. این امر قابل بازبایی است.

پیش از کاغذ

نیاز به برقراری ارتباط محرمانه با کسی در دوردست، قدیمی‌تر از نوشتن است. در بین‌النهرین، لوح‌های گلی حاوی پیام‌های اداری یا خصوصی درون کپسول‌هایی از جنس گل فرستاده می‌شدند که پیش از پختن مهر و موم می‌شدند: هرگونه تلاش برای خواندن محتوا مستلزم شکستن پوشش بود و گیرنده با یک نگاه می‌فهمید که آیا کپسول سالم رسیده است یا خیر. در رم کلاسیک، طومارهای پوستی با ریسمان بسته شده و با موم یا سرب مهر و موم می‌شدند. ایده همیشه یکسان بود: هرگونه مطالعه غیرمجاز باید اثری فیزیکی و پاک نشدنی بر جای بگذارد.

عصر مهر و موم

برای چندین قرن، از پایان قرون وسطی تا اوایل قرن بیستم، ابزار متعارف مکاتبات محرمانه در اروپا، کاغذ تاشده و مهر و موم شده با مهر و موم بود. موم مذاب روی محل اتصال برگه ریخته می‌شد و با یک مهر شخصی یا سازمانی روی آن نقش می‌بست. این کار تزیینی نبود. دفترداران، دیپلمات‌ها، تجار و افراد عادی با همان منطق از آن استفاده می‌کردند: اگر مهر و موم سالم بود و نقش مهر قابل شناسایی، محتوا خوانده نشده بود؛ اگر شکسته بود، مکاتبات حتی پیش از باز کردن به خطر افتاده بود.

قدرت مهر و موم نه در گران‌بها بودن و نه در رسمی بودن آن بود، بلکه در یک ویژگی ساختاری بسیار خاص نهفته بود: هرگونه تلاش برای برداشتن و دوباره گذاشتن آن، آثار مشهودی بر جای می‌گذاشت. هیچ راه بی‌صدایی برای باز کردن یک نامه مهر و موم شده وجود نداشت. و این بدان معنا بود که محرمانگی نه به قول هیچ واسطه‌ای - نامه رسان، درشکه‌چی یا مامور پست - بلکه به طراحی فیزیکی خود پوشش بستگی داشت. این اعتمادی بود که بر شواهد استوار بود، نه بر حرف دیگران.

انتقال دیجیتال

تلگراف، تلفن، پست الکترونیک، پیام‌رسانی سازمانی. ارتباطات الکترونیکی سرعت، گستره جهانی و هزینه‌ای تقریباً صفر برای هر پیام به همراه داشت. همچنین تضمین مهر و موم را نیز از میان برد. به طور پیش‌فرض، تمام پیام‌ها از واسطه‌هایی عبور می‌کنند که یکپارچگی آن‌ها را تنها از طریق وعده‌های نوشته شده در شرایط خدمات، گواهینامه‌های فنی و ممیزی‌های مبهم می‌توانیم بررسی کنیم. هیچ معادلی برای یک قطره موم شکسته وجود ندارد که به ما هشدار دهد.

یک مهر و موم دیجیتال

ویژگی‌ای که به مهر و موم قدرت می‌بخشید خود مهر و موم نبود، بلکه چیزی بود که نمایندگی می‌کرد: یکپارچگی قابل تایید از طریق طراحی، بدون نیاز به اعتماد به شخص ثالث. این ویژگی را می‌توان در سطح دیجیتال بازسازی کرد، اگرچه با دو عنصر به جای یک عنصر. اولی مهر رمزنگاری است - اثر SHA-256 که در پای هر مقاله از این نشریه ظاهر می‌شود، به معنای واقعی کلمه، یک مهر و موم دیجیتال است: هرگونه تغییر در محتوا، اثر را به وضوح

تغییر می‌دهد، درست همان‌طور که موم شکسته خواندن غیرمجاز را فاش می‌کرد. دومی معماری کانال است: وقتی بین دو نفری که با هم ارتباط برقرار می‌کنند سروری در میان نباشد، واسطه‌ای وجود ندارد که لازم باشد به او اعتماد کرد. ترکیب این دو عنصر - یکپارچگی قابل تایید و نبود واسطه - در دنیای دیجیتال همان کاری را بازتولید می‌کند که برای چهار قرن موم قرمز روی کاغذ تا شده به طور روزمره انجام می‌داد.

نام

نام این نشریه Cuadernos Lacre است زیرا مهر و موم یک تزیین تاریخی نیست، بلکه یک ویژگی فنی خاص است: یکپارچگی قابل تایید از طریق ساخت، بدون وعده هیچ اِپراتوری. هر مقاله از این مجموعه، در نسخه دیجیتال معاصر خود، بخشی از همان ایده را تحلیل می‌کند: رمزگذاری، متاداده، رازداری حرفه‌ای، معماری ارتباطات، چارچوب قانونی اروپا. این نام همچنین راهی است برای یادآوری اینکه محرمانگی خدماتی نیست که خریداری شود، بلکه ویژگی خود کانالی است که اطلاعات در آن جریان دارد.

منابع و مطالعه بیشتر

- ماکسول، ام. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*، روتلج، ۱۹۹۲ (فصل‌های مربوط به مهر و موم کردن لوح‌ها و بولاهای بین‌النهرینی).
- دیبل، جی. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*، پالگریو، ۲۰۱۲. فصل‌های مربوط به مهر و موم به عنوان ابزار یکپارچگی و اصالت.
- سالتزر، جی. اچ.؛ رید، دی. پی.؛ کلارک، دی. دی. — *End-to-end arguments in system design*، ACM TOCS، ۱۹۸۴. فرمول‌بندی مدرن اصل مهر و موم: تضمین در دو انتها، نه در کانال واسطه.

[التالي → رمزنگاری به معنای حریم خصوصی نیست: متادیتا درباره شما چه می‌گوید](#)

قراءات حدیثه

- [CUADERNOS LIST PREGUNTAS TITLE](#)
- [CUADERNOS LIST SELFHOST TITLE](#)
- [CUADERNOS LIST IDENTIDAD TITLE](#)

این مقاله را هر کجا که نیاز دارید همراه خود ببرید.

[↓ مارک‌داون ↓ متن ساده ↓ PDF](#)

فایل در دستگاه شما دانلود خواهد شد. از آنجا می‌توانید آن را ذخیره کنید، به Solo2 وارد کنید یا در هر کجا که می‌خواهید به اشتراک بگذارید. Cuadernos مقصد را برای شما تعیین نمی‌کند.

ختم شمعی · SHA-256 ae50c96494238663eebd94d28b113a48e92bf1a4b6cc4dea7bfd080758f1c0d7

ES

· [Menzuri Gestión S.L.](#) نشریه من · Cuadernos Lacre
· کتبه R.Eugenio · حررها فریق [Solo2](#).

این وبسایت از کوکی استفاده نمی‌کند و منابع شخص ثالث را بارگذاری نمی‌کند. این سایت از یک شمارنده بازدید ناشناس خود-میزبان (Umami، روی سرور اروپایی ما) و حداقل جاوا اسکریپت لازم برای تنظیم تم روشن/تاریک شما استفاده می‌کند. بدون ردیاب، بدون پروفایل‌سازی، بدون اشتراک‌گذاری داده‌ها. اگر می‌خواهید ما را دنبال کنید: [RSS](#).