Cryptomathic

Cryptomathic is a technology firm specializing in cryptology-related services. It boasts a variety of software products and provides services to the areas of banking, government, cloud-storage, and communications, among other domains.[1] A host of academics, researchers, and cryptographers have led or been involved in Cryptomathic's work since its founding in 1986, establishing the company's reputation as a pioneer in the field of cryptography.[2]

Cryptomathic's foremost products are steeped in an array of sophisticated cryptology algorithms. For example, its Authenticator server system utilizes CAP / DPA authentication standards, matrix cards, two-factor authentication algorithms, one-time password (OTP) features, and pattern learning.[3] Of particular interest here is Authenticator's incorporation of the HMAC-based OTP (HOTP) algorithm. This algorithm is a widely used cryptology protocol associated with the Initiative For Open Authentication (OATH), an open standards initiative within the cybersecurity sector.[4]

The HOTP algorithm involves a secret key, shared between both parties, and a counter variable. Using the key, a cryptographic hash function, namely a version of NSA's Secure Hash Algorithm, is applied to the counter variable using the key to generate a hash-based message authentication code, which can be used to encrypt communications. The counter variable is incremented to form new passwords in-between communications, hence the term *one-time password*.[5]

Cryptomathic implements HOTP in authentication servers as a means of authenticating users. As more advanced cryptology techniques develop, HOTP and its hash algorithm continue to improve and are increasingly augmented with other protocols. This protocol diversity is epitomized in banking applications, where HOTP and related protocols accompany a series of standard finance-related authentication systems such as MasterCard CAP, Visa DPA, Vasco Digipass, and others.[6] Thus, while any specific example of a cryptology algorithm, such as HOTP, is inevitably just one component of a complex and adaptive solution provided to players across many modern industries, it provides a glimpse into the nature of modern cryptography in both practice and research.

An impression of Cryptomathic's broader contributions to the domains of computer science and cybersecurity can be conveyed by synopsizing several of its and its members' many associated accolades. For example, Whitfield Diffie, who received the 2015 Turing Award along with Martin Hellman for developing the popular Diffie–Hellman key exchange algorithm, is an advisory board member of the company.[7] Central figures within the company have been commended by groups as diverse as the European Patent Office and the MIT Technology Review. The company itself was designated as a Technology Pioneer by the World Economic Forum in 2003, and in 2004 received VISA's Smart Start Award for its contributions to finance-related cryptography systems. As a central player in international financial security, in addition its many other roles, Cryptomathic will continue to play a central role in the future global economy.

Bibliography

[1] "About Us - Cryptomathic." Cryptomathic. Web. 28 Oct. 2016. <https://www.cryptomathic.com/company/about-us>.

[2] "Cryptomathic." Wikipedia. Wikimedia Foundation, Web. 28 Oct. 2016. <https://en.wikipedia.org/wiki/Cryptomathic>.

[3] "Authenticator." Cryptomathic.com. Cryptomathic, n.d. Web. 28 Oct. 2016. <https://www.cryptomathic.com/products/authentication-signing/authenticator-multi-factor-authentication>.

[4] "HMAC-based One-time Password Algorithm." Wikipedia. Wikimedia Foundation, n.d. Web. 28 Oct. 2016. <https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm>.

[5] Major, Peter. "One-Time Passwords – HOTP and TOTP." Aldaris' Blog. N.p., 28 Feb. 2014. Web. 28 Oct. 2016. <http://blogs.forgerock.org/petermajor/2014/02/one-time-passwords-hotp-and-totp/>.

[6] Cryptomathic Authenticator. Cryptomathic.com. Web. 28 Oct. 2016. <www.cryptographic.com>.

[7] "Cryptology Pioneers Receive ACM A.M. Turing Award." Acm.org. Association for Computing Machinery, 1 Mar. 2016. Web. 28 Oct. 2016. <https://www.acm.org/awards/2015-turing>.