Research the phrase “RSA-2048 cash prize” to discover why a company has a $200,000 reward for anyone who can find the factors of a large number. Explain how this reward relates to cryptography.

RSA-2048 is a type of asymmetric encryption algorithm widely used in securing communications over the internet. It relies on the difficulty of factoring the product of two large prime numbers, which forms the RSA modulus. The security of RSA is based on the assumption that factoring large numbers into their prime factors is a computationally infeasible task, especially when the numbers involved are very large.

A company is offering a $200,000 reward for anyone who can factor the large number used in RSA-2048 encryption. This reward relates to cryptography as it tests the security of RSA, which relies on the difficulty of factoring large numbers. If someone can efficiently factor the number, it could compromise the encryption's security. The steps involve generating large prime numbers, computing the modulus, selecting public and private keys, encrypting data, and the challenge of factoring for decryption. The cash prize incentivizes researchers to explore and uncover potential vulnerabilities in cryptographic systems.

References:

<https://www.theregister.com/2001/07/25/rsa_poses_200_000_crypto/>

<https://www.moodysanalytics.com/articles/2023/rsa-and-diffie-hellman-cryptosystems-under-threat-sooner-than-previously-thought>