International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Securing Digital Markets: The Economic Role of RSA Encryption and the Consequences of Security Failure

Vasishth Rungta

Abstract

The rapid expansion of digital markets has made secure communication an essential prerequisite for economic activity. Among the technologies that support this environment, the RSA encryption algorithm has become one of the most widely used public-key cryptographic systems, enabling secure online transactions, authentication, and digital communication. This paper examines the extent to which RSA encryption enables digital trust in online markets and analyses the economic consequences when digital security fails. It first outlines the mathematical foundations of RSA before exploring its role in reducing information asymmetry, lowering transaction costs, and supporting network effects that encourage consumer participation in digital commerce. The paper then evaluates the economic implications of implementation failures through prominent cybersecurity incidents, demonstrating how weaknesses in surrounding security infrastructure can lead to financial losses, reputational damage, and reduced consumer confidence. It argues that while RSA provides the cryptographic foundation necessary for secure digital markets, its effectiveness depends upon robust implementation, complementary security protocols, and institutional governance. Ultimately, RSA should be understood not only as a technical security mechanism but as a critical component of the economic infrastructure that enables trust, participation and efficiency within modern digital markets.

Keywords: RSA Encryption, Digital Trust, Digital Markets, Information Asymmetry, Cybersecurity Economics

Introduction

Every day, trillions of dollars move across digital networks through online banking, electronic payments, and e-commerce platforms (Cooper, 2016). These transactions occur over open networks like the internet, where it is very easy for an eavesdropper to intercept and steal sensitive data. Hence, a strong encryption system is essential for protecting sensitive personal and financial information. Digital markets function effectively only when users trust that their data and transactions are secure. Encryption and decryption play a foundational role in enabling safe digital interaction and supporting the growth of online economic activity. The RSA Algorithm, named after its inventors, Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, is a widely used public-key algorithm in many digital markets to ensure secure digital transactions and authentication (Simmons, 2020).

Although encryption systems like RSA are designed to secure digital transactions, security failures still occur due to weak implementation, outdated systems, or cyberattacks. These failures have led to significant economic consequences, including financial losses for firms, erosion of consumer trust, and disruptions in digital markets. **It has been predicted that by 2031, the cost of cybercrime will amount**

to $12.2 trillion, based on a steady 2.5 percent annual increase (Sausalito, 2026). This raises an important question about the broader economic role of encryption technologies: **To what extent does RSA encryption enable digital trust in online markets, and what are the economic consequences when digital security fails?**

RSA encryption functions not only as a technical security mechanism but also as a key component of the economic infrastructure in digital markets, as it supports authentication, confidentiality, and secure communication. It also helps reduce transaction risk and encourages consumer participation in online commerce and financial systems. However, when digital security mechanisms fail or are improperly implemented, the resulting breaches can produce high economic costs, including financial losses, reputational damage, and reduced consumer confidence. The paper will therefore argue that strong encryption systems, such as RSA, are essential for sustaining trust and efficiency in digital markets, and that weaknesses in digital security can have substantial economic consequences.

Technical Foundation: RSA Encryption

Early encryption systems relied on symmetric key encryption. Symmetric Key Encryption is a cryptographic method that uses the same secret key to encrypt and decrypt messages. Common Encryption Algorithms include Advanced Encryption Standard (AES) and Data Encryption Standard (DES). While this method can be effective, it creates a key distribution problem because the shared key must be transmitted securely before communication can begin. The shared key must be shared between the two members in an ideal world without eavesdroppers, but such ideal worlds do not exist; hence, in large digital networks such as the internet, securely exchanging keys between users who have never interacted before becomes difficult (Crane, 2020). Public key cryptography was developed to address this challenge by introducing a system that uses two keys, one public and one private, that are mathematically related. The public key is shared openly in the real world and can be used to encrypt messages, whereas the private key is known only to the owner and can be used to decrypt messages. This framework allows secure communication without requiring a pre-shared secret, making it particularly suitable for large-scale digital systems.

RSA is one of the most widely used implementations of public key cryptography. RSA generates a key pair consisting of a public key and a private key. Messages can be encrypted using the
public key, but they can only be decrypted using the corresponding private key. The RSA Algorithm consists of three steps:

1. **Key Generation –** This algorithm takes two 1024-bit prime numbers ∈ N and generates a public key and a secret key. Two large prime numbers p and q are taken, and their product is calculated as $n = p \times q$. The Euler's totient function of n is calculated, which is given by $\phi(n) = (p - 1)(q - 1)$. After that, an integer e is selected such that e is coprime with $\phi(n)$, meaning the greatest common divisor of e and $\phi(n)$ is 1. The last step is to compute d such that the product of e and d is congruent to 1 modulo $\phi(n)$. The pair (e,n) is generated as the required public key, while d is generated as the corresponding private key. The public key is the pair (e, n), and the private key is d.
2. **Encryption –** Algorithm that takes the public key pk = (n,e) and a message m and generates a ciphertext c by encrypting the message m. The ciphertext is calculated by calculating the modular exponent of m, i.e., c = m raised to the power e, modulo n.
3. **Decryption –** Algorithm that takes the secret key sk = d and the ciphertext c and generates the message m by decrypting the ciphertext c. The original message is again recovered by calculating the modular

exponent of c, i.e., m = c raised to the power d, modulo n (Jhanwar, 2023).

RSA is based on the mathematical difficulty of factoring large numbers. The security of RSA comes from the fact that while it's easy to multiply two large primes, it's extremely hard to reverse that and factor their product. Modern computers require a very long time to perform this calculation. When the numbers are sufficiently large (1024 bits, which corresponds to 309 decimal digits), it becomes practically infeasible for an attacker to derive the private key from the public key (Bhatt, 2024).

RSA plays a key role in securing internet communication through protocols such as SSL (Secure Sockets Layer) and TLS (Transport Layer Security), which protect data exchanged between users and online platforms. SSL is a foundational security technology that creates an encrypted link between a web server and a browser, ensuring data privacy and integrity (GeeksforGeeks, 2026), and TLS is a cryptographic protocol that secures data transmitted over networks, commonly enabling HTTPS to protect web traffic from eavesdropping and tampering (Jonker & Krantz, 2025). These protocols are widely used in systems such as online banking services, digital payment platforms, and e-commerce websites. RSA also supports functions such as digital signatures, hash-based authentication, and secure key exchange, which help verify user identities and ensure that data has not been altered in transit. By enabling these forms of protection, RSA helps create secure communication channels that support the functioning of modern digital markets.

Digital Trust as an Economic Asset

Trust is indispensable for social and economic relations; it is the glue that holds organizations together and seems to work in mysterious ways. Unlike traditional face-to-face transactions, online interactions involve uncertainty because users cannot directly verify the other party's identity or reliability. This creates a fundamental problem of trust, which can limit participation in digital systems such as online banking, e-commerce, and digital payments. Users in the economy must believe that their transactions are secure and that their financial and personal information will not be compromised for the digital market to function successfully. Trust is accordingly not just a social concept; it is also an economic requirement for people's participation in the market and its growth.

The economy is fundamentally a network of relationships built on mutual expectations. More than that, trust is the glue that holds civilization together. Trust and ethics really matter in society (Ho, 2021). Firstly, trust and ethics make all kinds of economic interactions easier in the private sphere by greatly reducing transaction costs, thereby promoting social cohesion. Governments also require public trust to enact public policy effectively. It is highly unlikely that pressing socioeconomic challenges will be solved in a society that is divided, distrustful, and lacks trust in the government. Lastly, trust and ethics are inherently critical for building economic cooperation in all its forms. Countries need to trust each other to establish international treaties; hence, governments also need the trust and support of their citizens regarding these treaties (Tharwat, 2024).

Information asymmetry is an economic phenomenon in which one party to a transaction possesses more information than the other, potentially leading to an imbalance in decision-making. This uncertainty raises transaction costs because users may have to spend more time verifying information, avoid certain platforms, or refuse to engage altogether (EBSCO, 2023). Secure systems, supported by technologies such as RSA encryption, help reduce this asymmetry by ensuring confidentiality, authentication, and data integrity. Secure systems enhance transparency and enforce accountability, which creates trust by making information reliable and accessible to authorized parties while restricting access to unauthorized parties.

As a result, transaction costs decrease, and market efficiency improves.

Digital trust offers a wide range of benefits that affect nearly every aspect of how an organization operates, interacts with customers, and maintains a competitive advantage in the digital economy. When companies demonstrate that they can protect data, respect privacy, and act transparently, the trust they inspire can drive measurable business value. It also increases consumer confidence and loyalty, strengthens brand reputation and customer engagement, and reduces cyber risks. When users trust a platform, they are more likely to participate in transactions, share information, and adopt new technologies. This increased participation leads to the network effect.

The network effect is a phenomenon in which the value of a product, good, or service increases as more people use it and share their experiences with others. This engagement contributes to a product's increased value and reach. Users can become product advocates, which helps spread awareness and drive sales growth for businesses (Banton, 2026). Secure encryption systems like RSA indirectly support this process by maintaining the trust that sustains user engagement. Secure systems like RSA protect a user's sensitive data, ensure business continuity, and prevent financial losses from potential cyberattacks. With a strong security system, a user's intellectual property and reputation are protected as well. Hence, without reliable and secure security systems, these network effects weaken, resulting in slower growth in the digital economy.

Economic Costs of Weak or Failed Digital Security

Despite the mathematical foundations that make RSA encryption theoretically robust, the practical deployment of cryptographic systems is far more vulnerable than their theoretical design suggests. Security failures rarely emerge from breaking the underlying mathematics of RSA itself; rather, they arise from weak implementation practices, outdated protocols, misconfigured systems, and, most consequentially, human error. A poorly generated prime number, an improperly stored private key, or an unpatched vulnerability in a communication protocol can unravel the entire security architecture that encryption is designed to provide. When such failures occur, sensitive personal and financial data becomes exposed, secure communication channels are compromised, and the authenticated trust relationships that RSA was specifically designed to establish break down entirely. It is critically important to recognize that these events are not simple technical malfunctions confined to the servers of affected organizations. They are, in a meaningful and measurable sense, economic events. A breach entails the destruction of information-asymmetry protections, the erosion of the trust infrastructure discussed in the previous section, and the introduction of substantial friction into digital markets that had previously functioned efficiently. The transition from examining the benefits of strong encryption to understanding the costs of its failure is therefore not merely an academic exercise; it is central to evaluating the true economic value of digital security as infrastructure.

The most immediately visible consequence of digital security failures is the direct financial damage sustained by organizations and their users. When encryption fails or is improperly implemented, attackers can intercept financial data, steal funds, or impersonate legitimate users to conduct fraudulent transactions. Beyond direct theft, organizations face substantial regulatory penalties under frameworks. In addition to regulatory fines, they must also absorb the operational costs of incident response, including forensic investigation, system remediation, cybersecurity infrastructure upgrades, and legal proceedings. These expenditures accumulate rapidly and often extend over months or years following the initial breach, placing considerable strain on organizational finances.

Several real-world vulnerabilities illustrate implementation failures. The Heartbleed Bug (2014) was a critical flaw in the OpenSSL cryptographic library that allowed attackers to read protected memory from servers, potentially exposing private keys and user credentials across approximately 17 percent of the internet's secure web servers (Durumeric et al., 2014). The ROCA vulnerability (2017), discovered in RSA key-generation code by Infineon Technologies, affected an estimated 760,000 cryptographic keys used in government-issued identity cards, smart cards, and enterprise devices, rendering those keys mathematically factorable and therefore entirely insecure (Nemec et al., 2017). The DigiNotar breach (2011) saw attackers compromise a Dutch Certificate Authority and fraudulently issue over 500 SSL certificates, including those for Google domains, enabling large-scale man-in-the-middle attacks before DigiNotar was ultimately forced into bankruptcy (van der Meulen, 2013). Each of these failures demonstrated that cryptographic security is only as strong as its weakest link in the implementation chain. The longer-term economic consequences of security failures extend well beyond the immediate financial losses and operate through a fundamentally behavioral mechanism. When users experience or learn of a significant breach, their confidence in the affected platform diminishes, and they reduce their engagement or exit entirely. This withdrawal of participation directly weakens the network effects discussed in the previous section. As active users decline, the platform's value diminishes for the remaining participants, potentially triggering a self-reinforcing cycle of disengagement that is extremely difficult to reverse. Reputational damage compounds this problem even after an organization has remediated its technical vulnerabilities; restoring consumer confidence is a slow and costly process. At a macroeconomic level, the cumulative effect of repeated and high-profile security failures is a systemic reduction in trust in digital markets as a whole. This manifests in the underutilization of digital services, reluctance to adopt emerging financial technologies, and a general slowdown in digital economic activity. In this way, the breakdown of encryption-backed trust undermines the benefits of secure systems and actively introduces inefficiencies and growth constraints in an economy increasingly dependent on digital infrastructure for its functioning.

Evaluation and Conclusion

This paper examined the extent to which RSA encryption enables digital trust in online markets and the economic consequences when digital security fails. The argument advanced throughout has been that strong encryption systems, such as RSA, are essential for sustaining trust and efficiency in digital markets, as they reduce information asymmetry and transaction risk while enabling network effects. However, weaknesses in implementation and surrounding security infrastructure can generate substantial economic costs, including financial losses, reputational damage, and reduced consumer confidence in digital markets.

RSA encryption occupies a foundational position in the architecture of modern digital markets. As the preceding sections have established, RSA enables three key economic functions: secure authentication, which verifies the identities of transacting parties; encrypted communication, which protects sensitive data in transit; and digital signatures, which ensure the integrity and non-repudiation of messages. Each of these functions directly addresses the problem of information asymmetry that characterizes online transactions. When a user interacts with a banking platform or an e-commerce service, they cannot directly verify the identity or reliability of the system they are engaging with. RSA resolves this uncertainty by creating a cryptographic basis for trust, reducing transaction risk and supporting the consumer confidence that sustains participation in digital markets. This trust is not merely a social or psychological condition but an

economic requirement, since users must believe their transactions are secure for digital markets to function and grow. When this trust is present, it drives the network effect, where increased user participation raises the value of a platform for everyone involved. In this sense, RSA is not just technically significant; it is economically significant because it enables trust-based exchange at scale, transforming what would otherwise be high-risk, friction-laden interactions into routine commercial activity.

However, a critical limitation must be acknowledged. RSA does not function in isolation, and digital trust is not produced by encryption alone. The security of a digital market depends on a broader ecosystem of interdependent components: the correct implementation of cryptographic protocols such as TLS, the integrity of certificate authority infrastructure, the adequacy of regulatory frameworks governing data protection, and the organizational cybersecurity practices of the platforms themselves. The real-world failures examined earlier demonstrate this point with precision. The Heartbleed vulnerability did not arise because RSA's mathematical foundations were broken; it arose because of a flaw in the OpenSSL library that exposed private keys stored in server memory. The ROCA vulnerability stemmed from defective key generation code in Infineon's hardware, which produced mathematically weak RSA keys despite the algorithm itself remaining sound. The DigiNotar breach compromised not the encryption standard but the certificate authority infrastructure that gives RSA-based certificates their economic meaning. In each case, the failure occurred in the implementation layer or the surrounding trust infrastructure, not in the underlying algorithm. This distinction is essential because it means that RSA can be cryptographically sound and economically ineffective simultaneously if the systems surrounding it are poorly designed, inadequately maintained, or improperly governed.

Weighing these two dimensions directly against each other, RSA enables digital trust to a significant extent. It provides the cryptographic foundation without which secure online communication, authentication, and financial transactions would be structurally impossible. By reducing information asymmetry and lowering transaction costs, it creates the conditions for digital markets to achieve the network effects and scale that drive economic growth. Yet its effectiveness is not unconditional. The trust that RSA generates is contingent on the reliability of the implementation practices, protocols, and governance structures that surround it. Where those systems are strong, RSA functions as genuine economic infrastructure. Where they are weak, its mathematical robustness offers little protection against the economic consequences of a breach. RSA is therefore necessary for digital trust in online markets, but it is not, on its own, sufficient to guarantee it.

Bibliography

1. Banton, C. (2026). *Understanding the Network Effect: How It Increases Product Value*. Investopedia. https://www.investopedia.com/terms/n/network-effect.asp
2. Bhatt, H. (2024, March 4). *What is RSA? How does an RSA work?* Encryption Consulting. https://www.encryptionconsulting.com/education-center/what-is-rsa/
3. Cooper, A. (2016). *ENCRYPTION: Securing Our Data, Securing Our Lives*. BSA. https://www.bsa.org/files/reports/BSA_encryption_primer.pdf
4. Crane, C. (2020, November 4). *Symmetric Encryption 101: Definition, How It Works & When It's Used*. Hashed out by the SSL Store™. https://www.thesslstore.com/blog/symmetric-encryption-101-definition-how-it-works-when-its-used/
5. Durumeric, Z., Payer, M., Paxson, V., Kasten, J., Adrian, D., J. Alex Halderman, Bailey, M., & Li, F. (2014). The Matter of Heartbleed. *Proceedings of the 2014 Conference on Internet Measurement*

Conference - IMC '14. https://doi.org/10.1145/2663716.2663755

6. EBSCO. (2023). *Information asymmetry* . EBSCO Information Services, Inc. | Www.ebsco.com. https://www.ebsco.com/research-starters/social-sciences-and-humanities/information-asymmetry
7. GeeksforGeeks. (2026, April 28). *Secure Socket Layer (SSL)*. GeeksforGeeks. https://www.geeksforgeeks.org/computer-networks/secure-socket-layer-ssl/
8. Ho, B. (2021). *Why Trust Matters: An Economist's Guide to the Ties that Bind Us*. Columbia News. https://news.columbia.edu/content/why-trust-matters-economists-guide-ties-bind-us
9. Jhanwar, M. P. (2023). *Computer Security and Privacy*. Google.com. https://sites.google.com/site/homeofmahavir/Home/computer-security-and-privacy?authuser=0
10. Jonker, A., & Krantz, T. (2025, July 7). *What is Transport Layer Security (TLS)?* Ibm.com. https://www.ibm.com/think/topics/transport-layer-security
11. Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017). *The Return of Coppersmith's A ack: Practical Factorization of Widely Used RSA Moduli *.* https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf
12. OECD. (2014). *Trust: What it is and Why it Matters for Governance and Education*. OECD. https://www.oecd.org/en/publications/trust-what-it-is-and-why-it-matters-for-governance-and-education_5jxswcg0t6wl-en.html
13. Sausalito, C. (2026, January 26). *Will The Cybercrime Economy Plateau In 2026?* Cybercrime Magazine. https://cybersecurityventures.com/will-the-cybercrime-economy-plateau-in-2026/
14. Simmons, G. J. (2020). RSA encryption | Britannica. In *Encyclopædia Britannica*. https://www.britannica.com/topic/RSA-encryption
15. Tharwat, I. (2024, January 14). *Why trust and ethics matter most in a turbulent economy*. World Economic Forum. https://www.weforum.org/stories/2024/01/trust-ethics-economics-governance/
16. van der Meulen, N. (2013). DigiNotar: Dissecting the First Dutch Digital Disaster. *Journal of Strategic Security*, *6*(2), 46–58. https://doi.org/10.5038/1944-0472.6.2.4