Chapter 3
Asymmetric Encryption

Christian Stohrer and Thomas Lugrin

3.1 Introduction

While symmetric encryption uses the same key to encrypt and decrypt data, public key cryptography uses a pair of keys. One of these keys is used for encryption and the other one for decryption. For the security of the public key cryptosystem, only the decryption key must be kept secret. For this reason, it is often referred to as the private key. On the other hand, the encryption key, or public key, can be made publicly available without harming the security of the cryptosystem.

3.2 Analysis

For a public key cryptosystem to be secure, it must be computationally infeasible to compute the private key from the public key [1]. As the processes for encryption and decryption differ from each other and rely on different keys, another name for public key encryption is asymmetric encryption.

Generally, one does not use public key cryptography to encrypt large amounts of data directly, as this is generally computationally more expensive than symmetric encryption. However, it is common to use public key cryptography to encrypt and securely exchange keys of symmetric encryption schemes (see Chap. 2). The symmetric keys are then used for bulk data encryption [1, 2]. This combination of public key cryptography and symmetric encryption is called hybrid encryption.

C. Stohrer · T. Lugrin (✉)
Federal Administration, Bern, Switzerland
e-mail: thomas.lugrin@vtg.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_3

To ensure that only the intended recipient can decrypt a cipher text, the public key must be authenticated through other means, e.g., a Public Key Infrastructure (PKI) [3]. For more information on key management, see Chap. 4.

Asymmetric encryption is not the only application for public key cryptography. Digital signatures, see Chap. 15, used to verify the authenticity of a document, are another important example. Another application is homomorphic encryption, see Chap. 8.

3.2.1 Definition

An asymmetric encryption scheme uses two different keys, a private one and a public one. While the public key is used for encryption and may be known by others, the private key is used for decryption and must be kept secret. Like most public cryptosystems, asymmetric encryption relies on one-way mathematical functions. This means that while it is easy to compute the result from given input data, it is hard to recover the input data from the result. Moreover, the corresponding mathematical problems are conjectured to be hard, such that it is computationally infeasible to decrypt a message without knowing the private key.

3.2.2 Trends

The widespread public critical systems are based on the integer factorization problem or the discrete logarithm problem over finite fields and elliptic curves. In a seminal paper, Peter W. Shor showed that it is possible to solve these problems efficiently using a sufficiently powerful quantum computer [4]. This triggered the search for replacement schemes. Several standardization agencies are now evaluating new proposals for this. In 2022, NIST announced the winners of their corresponding competition. For further details, we refer to Chap. 10 dedicated to post-quantum cryptography.

3.3 Consequences for Switzerland

The advent of the quantum computer threatens public key cryptosystems considered secure today. A strategy should therefore be developed that considers the implications of this threat on the security of current systems and proposes appropriate measures to ensure the preservation of security.

3.3.1 Implementation Possibilities: Make or Buy

Generally, one should not develop proprietary public cryptosystems, as the standardized algorithms have been thoroughly tested and deeply analyzed. Furthermore, any proprietary design will likely fail and expose weaknesses that may corrupt the entire system's security. Therefore, when procuring products involving public key cryptography, only those that have been standardized and verified for correctness by an appropriate specialized authority should be considered.

3.3.2 Variation and Recommendation

We recommend to continue using well-established public cryptosystems, e.g., RSA (Rivest-Shamir-Adleman cryptosystem [5]) with OAEP (Optimal Asymmetric Encryption Padding), Elgamal over a finite field, and Elgamal over appropriate elliptic curves. The minimal key length and the required size of the involved parameters should be chosen according to the current regulation or best practice advice. With today's knowledge, these algorithms are considered secure, although they are known to be vulnerable to future powerful quantum computers. Cryptosystems based on elliptic curves (ECC) can use shorter keys and are thus more efficient to achieve the same security level against attacks with classical, i.e., non-quantum computers. They should therefore be preferred over RSA and classical Elgamal. However, the above reasoning does not hold when considering attacks *against* a future large-scale quantum computer. In this scenario, one should not try to enhance security by using larger keys; one should instead use alternative quantum-safe cryptosystems, see Chap. 10.

In addition, one should follow the various standardization initiatives for new quantum-safe alternative public vital algorithms and integrate them accordingly to mitigate the threat posed by quantum computers. For this, a deep understanding of algorithms and a close inspection of possible solutions are necessary.

3.4 Conclusion

Asymmetric cryptography is a core part of many cryptographic applications. For example, it allows for encrypting messages, exchanging secret keys over an insecure channel, and establishing authenticity using digital signatures.

Current public cryptosystems are considered secure against classical computers (operating with bits), but the large majority of those commonly used today will be broken by attacks from not yet existing powerful quantum computers. Therefore, a corresponding strategy should be developed and implemented to counter this risk.

References

1. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, October 1996.
2. Wikipedia, Public-key cryptography. https://en.wikipedia.org/w/index.php?title=Public-key_cryptography&oldid=1099221204, July 2022.
3. Carlisle Adams and Steve Lloyd. *Understanding Public-Key Infrastructure*. Addison–Wesley Professional, Boston, 2nd edition, 2003.
4. Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997. arXiv:quant-ph/9508027.
5. R. L. Rivest, A. Shamir, and L. Adleman. a method for obtaining digital signatures and public-key cryptosystems. 21(2):120–126, feb 1978.