### Decryption with the RSA Algorithm

Decryption works similarly to encryption:

We look at each number c of the ciphertext and apply the following formulacdmodM

We reassemble the decoded numbers into a sequence of numbers.

Then we use the table again to translate the decoded numbers back into letters. This way we get the original plain text.

The following example will illustrate this process.

Let (d, M) = (47, 143) be the private key we calculated in the key generation example Example: Decryption with the RSA algorithm

above. Please note that we do not need the public key for decryption.

We decode the ciphertext

21. 0 110 110 First, we apply the formula sequence. We receive:27 cd mod M = c47 mod 143 to each number c in the

2. The decoded sequence of numbers is therefore2711011020474747mod143 = 7mod143 = 04747mod143 = 14mod143 = 11mod143 = 11

70 11 11 14

We translate this sequence of numbers with the table back into a sequence of letters and get as plain text Hallo

As you can see, the RSA procedure is quite easy to apply. The greatest difficulty lies in generating the keys. Once these are constructed, the numbers can easily be inserted into the formulas for encryption and decryption and calculated. Please note that in the above examples we have chosen very small prime numbers for illustrative purposes. In practice, much larger numbers are used to increase the security of the system.

The RSA algorithm as described, often known as “textbook RSA,” contains a serious security weakness since the same clear text always results in the same cipher text. In the example above this can be seen in the fact that both instances of the letter “l” in “Hallo” were encrypted by the same cipher text “110.” In practice, one does not encrypt single characters as done in the example, but uses an entire string as the message z to be encrypted. Nevertheless, the basic problem remains that repeatedly encrypting the same clear text will result in the same cipher text.

This property allows a number of different attacks. Furthermore, even if an attacker only knows that the same message (part) was sent repeatedly, this may provide important information, without being able to decrypt the message. To protect against such attacks, we need to modify the RSA algorithm in such a way that repeated messages cannot be recognized as such by an attacker. The standard approach to achieve that is to use some form of “padding” the message, i.e. before encrypting the message, it is extended by adding random characters following defined rules. The receiver can then remove these random characters after decrypting the message.

LIST OF REFERENCES

Aigner, M. (2006). Diskrete Mathematik [Discrete mathematics] (6th ed.). Vieweg + Teubner Verlag. https://doi.org/10.1007/978-3-8348-9039-9

Alford, W., Granville, A., & Pomerance, C. (1994). There are infinitely many Carmichael numbers. Annals of Mathematics, 139(3), second series, 703—722. https://doi.org/10.2 307/2118576

Beutelspacher, A. (1994). Cryptology (C. J. Fisher, Trans.). The Mathematical Association of America.

Beutelspacher, A. (2003). Lineare Algebra. Eine Einführung in die Wissenschaft der Vektoren, Abbildungen und Matrizen [Linear algebra: An introduction to the science of vectors, maps, and matrices] (6th ed.). Vieweg + Teubner. https://doi.org/10.1007/978-3-8348-9 036-8

Beutelspacher, A. (2014). Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen [Cryptology: An introduction to the science of encryption, masking, and concealment] (10th ed.). Springer Spektrum. https://doi.org /10.1007/978-3-658-05976-7

Buchmann, J. (2003). Einführung in die Kryptographie [Introduction to cryptography] (3rd ed.). Springer. https://doi.org/10.1007/978-1-4419-9003-7

Euclid. (2003). Die Elemente [The elements] (4th ed.). Harri Deutsch.

Forster, O. (2017). Analysis 1. Differential- und Integralrechnung einer Veränderlichen (Grundkurs Mathematik) [Analysis 1: Single variable differential and integral calculus]

(12th ed.). Springer Spektrum. https://doi.org/10.1007/978-3-658-00317-3

Heuser, H. (2009). Lehrbuch der Analysis [Analysis textbook, part 1] (17th ed.). Teubner.

Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners. Springer. https://doi.org/10.1007/978-3-642-04101-3

Schneier, B. (2017). Applied cryptography: Protocols, algorithms and source code in C (20th ed.). Wiley.

Timmann, S. (2006). Repetitorium der Analysis [Review of analysis, part 1] (3rd ed.). Binomi.

Warner, S. (2019). Abstract algebra for beginners. Get 800.

Wiebe, H., & Storch, U. (2009). Lehrbuch der Mathematik, Band 1, Analysis einer Veränderlichen [Textbook of mathematics, volume 1, variable analysis] (3rd ed.). Spektrum. 160

Wiebe, H., & Storch, U. (2010). Lehrbuch der Mathematik, Band 2, Lineare Algebra [Textbook of mathematics, volume 2, linear algebra] (2nd ed.). Spektrum.

161