Cryptography and number theory in the classroom -- Contribution of cryptography to mathematics teaching

Katharina Klembalski
Institute of Mathematics, Humboldt-Universität zu Berlin, Berlin, Germany klembals@math.hu-berlin.de

Abstract
Cryptography fascinates people of all generations and is increasingly presented as an example for the relevance and application of the mathematical sciences. Indeed, many principles of modern cryptography can be described at a secondary school level. In this context, the mathematical background is often only sparingly shown. In the worst case, giving mathematics this character of a tool reduces the application of mathematical insights to the message ”cryptography contains math”. This paper examines the question as to what else cryptography can offer to mathematics education. Using the RSA cryptosystem and related content, specific mathematical competencies are highlighted that complement standard teaching, can be taught with cryptography as an example, and extend and deepen key mathematical concepts.

Introduction

Cryptography fascinates. Concepts such as secrecy, espionage, code cracking are often associated immediately (and not only among students). Hence, the motivation to work on this topic is high.
Modern cryptographic methods in particular are based in large parts on elementary number theory and are therefore accessible to secondary school students. Corresponding publications may be found both in mathematical as well as in computer science education literature (e.g., [1], [2]). An implementation into teaching practice in Germany is currently found predominantly in computing rather than in mathematics classes. This has effects on the nature and extent of the mathematical foundations presented. These often take a back seat in favor of the (partial) implementation of individual algorithms. Similar approaches for teaching specific mathematical content by means of cryptography that go beyond the pure cryptographic algorithms or protocols are rare and are often only implicit contained (typical [3], exception [4]). In this way, essential mathematical potential remains unused.
To show which contributions cryptography can make at school, the paper first introduces cryptography-related, general educational objectives which can be associated primarily with media competency and do not necessarily require mathematical expertise. The paper will then discuss the added value of considering cryptography within mathematics. The main focus is on the encounter with unsolved problems in mathematics, on the experience of mathematics as a living science as well as on cryptography as an application of mathematics. These considerations will be linked exemplarily to the RSA cryptosystem and its mathematical background. Finally, the paper outlines how this approach to cryptology deepens and extends known key mathematical concepts.

Why cryptography in school?

Due to the increase in electronic data traffic, cryptography is of practical relevance to everyone – be it through online banking, e-mails, electronic health cards, electronic passports or the protection of personal data. Within these applications, cryptography not only ensures the secrecy of data exchanged but also provides reliable means for the authentication of communication participants and for the verification of the integrity of data. Hence, as an element of media competency, students should acquire basic knowledge on the use of cryptographic applications.
General learning objectives in this regard are:

- raising awareness in relation to data security, especially the knowledge that data exchanged on the Internet can in principle be monitored and is thus insecure;
- derived from this, the insight into the necessity of encryption and the ability to perform and verify encryption;
- the knowledge that and how the identity of communication participants may be verified;

Integration of cryptography into the school curriculum differs among the German federal states as different standards exist in each state. Nevertheless, none of these contents are mandatory for all students, as cryptography in mathematics is only an elective subject. At junior secondary level, these elective subjects are usually found in years 9 or 10 and predominantly feature applications from classical cryptography (historical symmetrical ciphers like Caesar and Vigenère cipher). At senior secondary level, cryptographic content is almost exclusively taught in computer science. The guidelines here range from non-binding references to cryptography up to teaching units containing essential principles of modern cryptographic algorithms. Exceptions are the so-called “Seminarkurse”, which can be taken as elective courses in the Abitur (mandatory in Bavaria but voluntary in other federal states). The schools set up such courses according to their capacity in subjects that are in demand. The content of these courses may be chosen rather freely compared to standard courses in the

subject. The author of this paper taught such courses (2 semesters, 3 hours per week) in cryptography and number theory in 2007/2008.

Why cryptography in mathematics?

To give students an authentic image of the mathematics as a science, it is necessary to show current developments in scientific maths [5]. In this sense, cryptology[1] is a lucky coincidence [6, p. ix] as many of its modern techniques and algorithms can be fully explained and require little mathematical background (predominantly elementary number theory) in order to be understood. In the following, the example of the RSA cryptosystem and some closely related subjects are used to demonstrate how to extend the image of mathematics acquired in secondary school education.

a. Unsolved problems in mathematics

The contents of school mathematics do not extend beyond the scientific knowledge of the 18th century, with the exception of probability theory and some formalities. The contents of the classical branches of school (mathematics, arithmetic, algebra, calculus and geometry) may be found under the broader terms arithmetics and geometry as early as 1905 and have been intensely formed out and worked on since then [7]. Hence, the opportunity of having the students face unsolved scientific problems hardly exists within the scope of the standard mathematics curriculum. This fact has a very practical reason: Most of the open scientific questions within the aforesaid branches are difficult to describe at school level and thus hardly accessible to the student. Some open questions within other branches such as discrete mathematics, number theory or numerics are understandable, but the curriculum does not offer chances of a natural encounter with such issues. Therefore, it is advisable to take advantage of this when teaching cryptography.

Unsolved problems in number theory include, for example:

(1) Is there an infinite number of prime twins?
(2) Is there always a prime between n^2 und $(n+1)^2$?
(3) Is there an efficient way to find the prime factors of large numbers?

The first two questions are easy to grasp and are accessible by experimentation. They appear in connection with the distribution of prime numbers. [2]

The third question is particularly interesting from a cryptographic point of view. Consider the function E with $E(x) = x^e \pmod n$ where n and e are natural numbers, and n is large. As long as it cannot be answered in the affirmative, the function E may be seen as a one-way function, i.e. a function which is *practically* impossible to invert.[3] *Theoretically,* the inversion is solvable, because of the congruence $c = x^e \pmod n$ – for example by testing all x with $x = 1, 2, ..., (n-1)$. In practice, there is no efficient approach to this problem for large moduli n. The computation of x from e and n is equivalent to the knowledge of the prime factor decomposition of n ([8], p. 141). If n is chosen as a product of large, secret primes, the function cannot efficiently be inverted without this additional information. This fact is used in the construction of the RSA cryptosystem (see below).

The inability to solve (3) in this case represents no flaw but is essential to the security of the function E used in the RSA cryptosystem.[4] This gives the students the opportunity to deepen their understanding of integers in the context of cryptography and lets them experience that mathematical science is still incomplete. Additionally, the utilization of lack of knowledge supports a sparsely used approach in students' school experience.

b. Mathematics as a living science.

Cryptography has been used for several thousand years ([9], p. 105). A significant problem had always been the key exchange.[5] The solution to this problem was found approximately 30 years ago – namely by use of

[1] This text does not distinguish between cryptography and cryptology. Formally, cryptology is often used as an umbrella term which encompasses cryptography (science of designing ciphers) und cryptanalysis (art of breaking cipher systems).

[2] Questions on the existence and quantity of large primes arise for example when choosing suitable moduli n in the calculation of the function E described below. An estimate can be determined in the classroom with the use of the prime counting function π, where $\pi(n)$ denotes the number of prime numbers up to n, and its approximation by $n/\ln(n)$. To get an additional impression of the distribution of primes, the theorem on arbitrarily long prime gaps is available.

[3] The one-way property of a function arises from *experience*. To date there is no one-way function for which a proof of this property is known, i.e. the proof of the non-existence of an analytical inversion.

[4] Similar considerations apply to other functions, i.e. there is no general approach for calculating the discrete logarithm for large moduli n, which is exploited for cryptographic applications (Diffie-Hellman key agreement, ElGamal) ([8] p. 153).

[5] Until 30 years ago, information was encrypted solely according to the following principle. A message M is encoded by an invertible function E and a secret key K into a cipher text $C = E(M)$. The recipient decodes/decrypts the message with the inverse function D so that $D(C) = M$. The parameter K for the construction of E and D must be transmitted via a secure channel (personally in advance, by a courier, etc.). Secure data exchange between strangers (e.g. online shop and customer) over an insecure communication channel (internet) is not possible in this way.

mathematical knowledge that was already several hundred years old. Why so late?
The rise of computers and with it the new applications of cryptography were crucial for this development. The predominant historic use of cryptography had been the exchange of military secrets between two parties. In contrast, the use of computers increased in particular the exchange of sensitive data over multi-party communication networks. New tasks that had to be solved were the authentication of communication participants and the verification of the integrity of transmitted data.
In 1976 Diffie and Hellman published the idea of a public key algorithm which overcame the old key exchange problem [10]. An algorithm that implements this idea was published by Rivest, Shamir and Adleman in 1978 [11] and is known as the RSA cryptosystem. It is mainly based on Euler's theorem[6], which allows the generation of the keys $K_E = e$ for encryption and $K_D = d$ for decryption. From the knowledge of one of the keys one cannot derive the other, therefore K_E can be transmitted via a public channel (hence the name: public key algorithm). The key exchange problem has thus been solved.
Crucial to the effective application of the RSA cryptosystem was its simple computational implementation. Encryption and decryption (exponentiation with exponents e and d modulo n) as well as the key construction (determination of e and d) can easily be performed by square & multiply or the extended Euclidean algorithm.
The computer is thus tool and at the same time the occasion for the application of classical number theory in cryptography. This makes cryptography and the RSA cryptosystem a suitable example for pointing out the development in scientific mathematics triggered by the use of computers. This very direct link between application and mathematics is also an important fact which can extend students' perception of mathematics.
Computational mathematics, in particular numerical methods and discrete mathematics, has increased in importance in recent decades. A major contribution of the computer consists in shifting problems from computability to the development and implementation of suitable (and in particular efficient) algorithms. On the other hand, computers introduced new problems, such as the need for data compression (information theory).
Such developments are typical in the history of mathematics. They are often triggered by questions posed by other sciences, technological advances or even social developments. Physics and its influence deserve a particular mention here, for example for its influence on the development of calculus (mechanics), functional analysis (quantum mechanics) or differential geometry (general theory of relativity). This interrelation appears in teaching practice especially in the context of calculus. Demonstrating that such processes also take place today does, however, require a move beyond the standard curricula. Cryptography offers an opportunity to do so and can broaden the students' view of mathematics as a living science that is still developing.

c. Cryptography is applied mathematics

More to the point, modern cryptographic algorithms, and especially the RSA algorithm, are based on very old mathematics: mostly basic number theory, a branch of mathematics long known for its beauty rather than practical use. Essential elements like modular arithmetic, the Euclidean algorithm (at least 4th century BC) or Euler's theorem (18th century) were already valuable instruments within mathematics before their joint *practical* applicability for the RSA algorithm was recognized and became accessible through the use of computers. The application of mathematics in this case can be seen as an interdisciplinary transfer of mathematical knowledge to contexts other than those in which the insights were obtained.
The question arises as to which role the presentation of this transfer could or should have in the implementation of teaching. Number theory is, at least in Germany, not part of the curriculum. Its basics are generally only provided in connection with cryptography – usually simplified and isolated from the mathematical context. The depth of this presentation also depends on the temporal extent of the teaching unit and the weighting of cross-disciplinary relations, and primarily aims at providing an understanding of the cryptographic principles. This cannot be considered an application of existing knowledge. In the worst case, mathematics is reduced to an auxiliary science which permits the implementation of ingenious ideas seemingly by chance. What remains is cryptography and the insight "everything has maths inside".
That said, an extensive education in number theory and group theory at school is not feasible. However, the value of the mathematical content used should be made a topic beyond its cryptographic use. Otherwise,

[6] Euler's theorem was first proven by Euler in the context of modular arithmetic and later generalized to finite groups (G): Let gcd(a, n) = 1, then $a^{\varphi(n)} \equiv 1 \pmod{n}$, where φ is the Euler phi-function. I.e. φ(n) gives the number of nonnegative integers which are prime to n. In the case $n = pq$ the theorem can be simplified to $a^{(p-1)(q-1)} \equiv 1 \pmod{n}$. It follows $a^{k(p-1)(q-1)+1} \equiv a \pmod{n}$ for nonnegative integers k. Hence, for $ed = k(p-1)(q-1)+1$ the function E with $E(x) = x^e \pmod{n}$ presents a one-way function. This function can only be inverted (decrypted) with the knowledge of either d or p and q using D with $D(x) = x^d \pmod{n}$.

there is a risk that the problem solving appears arbitrary. Number theory should thus be connected with contexts beyond cryptography to illustrate its wider significance and use. Links to known curricular material but also to overarching contents are useful here. Examples:

- modular arithmetic: (i) Subsequent justification of the divisibility tests for 3 and 9 known from earlier years at school; (ii) Generalization of the proof technique known from differentiating between the cases "even" / "odd" for various moduli *n*; (iii) Outlook / consolidation: (**Z**/*n***Z**)* as one of several groups on which one-way functions can be defined; [7]
- Euclidean algorithm: (i) Comparison of the effectiveness of determining the gcd by comparing the prime factors (known in connection with the introduction of fractions) with that of the Euclidean algorithm; (ii) Outlook / consolidation: computation of multiplicative inverses in (**Z**/*n***Z**).
- Euler's theorem: Outlook / consolidation: order of group elements.

Conclusion

Cryptography is suited to exposing the students to unsolved questions in mathematical science in an authentic context (a). At the same time, it is an example that counters the common student perception that mathematical knowledge is a fixed structure and only has to be extended (b). Instead, mathematics appears as a science which vividly generates new branches and is engaged in a constant exchange of ideas with practical applications. These in turn arise from applications of knowledge already gathered and are interlinked with them in multiple ways (c). This is partially transferable to the classroom as cryptography is not independent of conventional classes but extends and deepens the pre-existing knowledge and perceptions of mathematics. This concerns in particular the key mathematical concepts[8] of *number* and *algorithm* and, depending on the implementation in the classroom, the concepts of *functional relationship* and *data analysis and probability*.

Key concept *number*: The knowledge of natural numbers is deepened. The occasion for this are questions of key construction for the RSA algorithm and its security. These lead to primes, their distribution, prime number tests and the problem of the factorization. In addition, familiar divisibility tests are proven with the help of modular arithmetic and are thus legitimized retrospectively. In particular, this presents an opportunity to highlight elementary unsolved problems in mathematics.

Key concept *algorithm*: The question of the key generation leads to the Euclidean algorithm, which the students can discover themselves. This and the square & multiply algorithm illustrate the advantages of algorithmic problem solving; questions about the efficiency of algorithms will arise almost by themselves. The importance of computer use for the application of these and other algorithms can be connected with the history of cryptography. This contrasts with the normal use of algorithms in secondary school, which is usually limited to solving systems of equations or, in the wider sense, to the processing of calculus problems (curve sketching).

Key concept *functional relationship*: The concept of the one-way function required in cryptography augments the invertible (if only by limiting their domain) function types already known. Furthermore, if the topic is covered in depth, students get to use the functions φ and π from number theory as two functions without closed expression.

Key concept *data analysis and probability*: the internal link to probability theory within mathematics originates, among others, from the need for suitably large primes for the key construction in RSA. The comparison of the probabilistic prime number test (Miller-Rabin test [8], p. 128) to the classic test for divisibility of all primes smaller than the square root of a candidate *p* is of interest in this context. Another opportunity to dig deeper concerns the construction of (pseudo-) random numbers used in conjunction with the security of the RSA algorithm.

The author investigates as part of her thesis how these ideas may be implemented in practical teaching. An example of the content and related key concepts for a practical implementation may be found in the appendix. The example refers to the first semester of a two-semester Seminarkurs in mathematics at senior secondary level.

Bibliography

[1] WITTEN, H. and SCHULZ, R.-H.: RSA & Co. in der Schule. Moderne Kryptologie, alte Mathematik, raffinierte Protokolle. Neue Folge – Teil 1: RSA für Einsteiger. *Log In* 23, No. 140 (2006), 45-54.

[2] GALLENBACHER, J.: *Abenteuer Informatik*. Spektrum Akademischer Verlag, Heidelberg 2008.

[3] MEYER, J.: Einblick in die Kryptographie. In: *ISTRON – Materialien für einen realitätsbezogenen Unterricht*.

[7] A similar consolidation is recommended to experience, that the property of being a one-way function is not bound to (**Z**/*n***Z**) and exponentiation. For example, cryptographic techniques which base their one-way property on the difficulty of inverting the discrete logarithm within (**Z**/*n***Z**) may be realized on elliptic curves - e.g. Diffie-Hellman Key Exchange ([8] p. 153).

[8] The notion of the key concept (Leitidee) is used here in the same sense as in the framework curriculum for senior secondary level mathematics in Berlin ([12], Kap.2). It combines the mathematical competencies to be acquired in school into competency areas. There is a distinction between process-related competency areas (reasoning and proof, problem solving, modeling, representation, use of procedures and tools, communication and cooperation) and key mathematical concepts (functional relationship, approximation, geometry, data analysis and probability, measurement, algorithms). The key concept "number" is, in contrast to the corresponding curriculum for the first 10 years of schooling, no longer listed as no specific content on extensions of numbers or the concept of numbers is included.

Bd. 6, 151-157. Franzbecker, Hildesheim 2000.
[4] EPKENHANS, M.: Die Kryptologie im Mathematikunterricht als Ideengeber für Facharbeitsthemen. *math.didact.* 25, No. 1 (2002), 17-36.
[5] LOVÁSZ, L.: *Trends in mathematics, and how they change education*. Invited talk, GDM 2008, Budapest
[6] BEUTELSPACHER, A.: *Kryptologie*. Teubner, Wiesbaden 2009.
[7] Meraner Lehrplan für Mathematik (1905). In Felix Klein: *Vorträge über den mathemati- schen Unterricht an den höheren Schulen.* (Teil 1, S. 208-220). Teubner, Leipzig 1907.
[8] BUCHMANN, J.: *Einführung in die Kryptografie*. Springer, Berlin 2007.
[9] BAUER, F. L.: *Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie*. Springer Berlin, 2000.
[10] DIFFIE, W. and HELLMAN, M.: New Directions in Cryptography. *Trans. IEEE Inform. Theory*, IT-22, 6 (1976), 644-654.
[11] RIVEST, R.L., SHAMIR, A. and ADLEMAN, L.: A method for obtaining digital signatures and public-key cryptosystems. *Comm. A.C.M.* 21 (1978), 120-126.
[12] SENATSVERWALTUNG FÜR JUGEND, BILDUNG UND SPORT: *Rahmenlehrplan für die gymnasiale Oberstufe Mathematik.* Berlin 2007.
[13] REMMERT, R. and ULLRICH, P.: *Elementare Zahlentheorie*. Birkhäuser, Basel 2008.

Appendix

Content	Key mathe-matical concept	Unsolved problems in mathematics		
			Mathematics as a living science. (Focus: algorithm)	
				Cryptography is applied mathematics
Classical cryptography				
- History and basic expressions - Key exchange problem			x	
Number theory				
Divisibility - Gcd, Euclidean algorithm (EA) - Bézout's lemma **(**incl. proof) /extended EA - Numeral system in different bases	N N/A A N		x x	x x
Primes - Proof: infinity prime numbers - Sieve of Eratosthenes - Distribution of primes, Prime number theorem (without proof) - Fundamental theorem of arithmetics	 N N/A N/F/A N	x	x	 x
Modular arithmetics - Calculation rules - Exercise: proof of divisibility tests of 3 and 9 - Fermat's little theorem (incl. proof) - Fast exponentiation: square & multiply algorithm	 N N N N/A		 x	 x x x
Modern cryptography				
Principles of public-key cryptography	F		x	
- RSA – principle (experimentation with CAS) - RSA – key generation (extended EA)LA - RSA – proof of correctness - RSA – for authentication	N/F A N N/F	x	x	 x x x
- *Primality tests* - *Chinese remainder theorem– fast signature* - *Attacks on RSA* - *RSA – on a debit card: weaknesses in the implementation* - *Factorization: quadratic sieve.*	N/A/DR N N/DR N N	 x	 x 	x x x

Table: Core topics for the first semester.

Optional topics prepared and presented by the students are shown in italics. This allows both for the variety of possible in-depth topics as well as for personal interest of students and teachers. On the other hand, it serves as a preparation for writing an extensive assignment at the end of the second semester of the Seminarkurs.