Schedule: Monday and Tuesday, 08.30-10.30. DUAL. Room 1BC50, Torre Archimede. First Lecture: September 27th. Last Lecture: December 20th.

Trial dates: to be communicated. **Remark**: The main references are [14] (in Italian) and the Addenda [13] (partly in Italian and partly in English). People coming from abroad can also use the references listed at the bottom of the daily summaries or at the end of every single topic (mainly Koblitz [9] and Knopse [8]).

TOPICS

WEEK 1.

Lecture 1 (09/27/2021). Overview. First definition of a Cryptosystem. Classical and Modern Cryptosystems. Enciphering and Deciphering keys and their role in the classification. Example: Caesar's method. Heuristics about RSA. Overview of the RSA method. (Ref. Koblitz [9])

Lecture 2 (09/28/2021). Definition of a bit operation. Computational complexity of sum, difference, product and division of two integers. Computational complexity of the product of $s > 2$ integers. (Ref. Koblitz [9])

WEEK 2.

Lecture 3 (10/04/2021). The Square and Multiply Method (to compute a^m and $a^m \bmod n$) and its computational complexity. Pseudocode for the Square and Multiply Method. (Ref. Koblitz [9]). Computational complexity of computing $(x+b)^n \bmod (x^r-1, n)$. (Ref. Granville [6] + AKS paper [1]).

Lecture 4 (10/05/2021). How to use Bezout formula to compute modular inverses. Computation of the b-expansion of an integer. The cost of computing the order of an element of a group. (Ref. Koblitz [9])

WEEK 3.

Lecture 5 (10/11/2021). How to use the Bezout formula to compute the solution of the Chinese Remainder Theorem. The Euclidean Algorithm. The length of the loop of the Euclidean Algorithm. Lemma about the rate of growth of the quotients of the Euclidean Algorithm. The Extended Euclidean Algorithm. The length of the loop of the Extended Euclidean Algorithm. Definition and some properties of the sequences a_k, b_k of the Extended Euclidean Algorithm. Computational complexity of the Euclidean Algorithm (Ref. Shoup [18] and Koblitz [9]).

Lecture 6 (10/12/2021). Computational complexity of the Extended Euclidean Algorithm (Ref. Shoup [18]). Basic algorithms: square root of n and its computational complexity; d-root of n and its computational complexity. How to verify that n is an integral power; its computational cost. (Ref. Shoup [18] and Koblitz [9]).

WEEK 4.

Lecture 7 (10/18/2021). Definition of the Euler totient function. On the Euler totient function: $\sum_{d|n} \varphi(d) = n$ and φ is a multiplicative function. $\varphi(n) = n \prod_{p|n}(1-1/p)$. RSA: $\varphi(n_X)$ has to be kept secret; the cost of getting p_X, q_X knowing $n_X, \varphi(n_X)$. (Ref. Koblitz [9]) Square roots of 1 modulo a prime. Square roots of 1 modulo $n = pq$, p, q distinct odd primes. (Ref. Koblitz [9])

Lecture 8 (10/19/2021). Wilson's Theorem; statement and computational remarks. A direct proof of Fermat Theorem. Pseudoprimality, remarks on Carmichael numbers and their distribution. The Miller-Rabin Theorem; computational remarks (Ref. Koblitz [9]).

WEEK 5.

Lecture 9 (10/25/2021). The Miller-Rabin Theorem; proof. Strong pseudoprimality. Proof of the Miller-Rabin theorem. Miller-Rabin probabilistic primality algorithm, its pseudocode. Assuming GRH, the Miller-Rabin method becomes a deterministic polynomial primality test (not proved). Computational complexity of the Miller-Rabin test. (Ref. Koblitz [9]). Remarks on the Riemann Zeta function and RH (Part 1: this will not be asked during the exam).

Lecture 10 (10/26/2021). Remarks on the Riemann Zeta function and RH (Part 2: this will not be asked during the exam). The Agrawal, Kayal, Saxena (AKS) Theorem (not proved). First remarks on the AKS Theorem. The AKS Algorithm and its correctness. Lemmas used to prove the computational complexity of the AKS algorithm (first part). (Ref. Granville [6] + AKS paper [1]).

WEEK 6.

Lecture 11 (11/02/2021). The AKS Algorithm and its correctness. Lemmas used to prove the computational complexity of the AKS algorithm. Computational complexity of the AKS algorithm (Ref. Granville [6] + AKS paper [1]).

WEEK 7.

Lecture 12 (11/08/2021). Eratosthenes' Sieve: description. Computational complexity of Eratosthenes' Sieve. Analytic tools to estimate the computational complexity of Eratosthenes' Sieve. (Ref. Crandall Pomerance [5]) Factoring algorithms: Trial division method for factoring integers. Fermat factoring method. (Ref. Koblitz [9])

Lecture 13 (11/09/2021). Comments about the Birthday Paradox. The Birthday Paradox. (Ref. Stinson [20, §4.2.2]) Factoring algorithms: Pollard's ρ method (and Floyd iteration); pseudocode; comments on the memory occupation. (Ref. Koblitz [9] and Pomerance [16])

WEEK 8.

Lecture 14 (11/15/2021). Pollard's $p-1$ method. Kraitchik idea on factoring. Remarks on Pomerance's Quadratic Sieve factoring method. (Ref. Koblitz [9] and Pomerance [16]). Few words on the digital signature. Definition of Digital signature using a public-key method; simpler case. (Ref. Koblitz [9])

Lecture 15 (11/16/2021). Definition of Digital signature using a public-key method: digital signature with message integrity. Hash functions and digital signatures. (Ref. Koblitz [9]). Digital signature using RSA. (Ref. Koblitz [9]) Attacks to RSA: $n_A = n_B$, chosen-ciphertext attack to RSA, broadcast attack (e "small") [first part]. (Ref. Boneh [2], Hinek [7])

WEEK 9.

Lecture 16 (11/22/2021). Attacks to RSA: broadcast attack (e "small") [second part]. Random Faults (Ref. Boneh [2], Hinek [7]; for the Pentium bug, see Cipra-Zorn [4])). Block Ciphers: definition and historical examples. Transmission methods: ECB, CBC.(Ref. Stinson [20], Buchmann [3])

Lecture 17 (11/23/2021). Transmission methods: CFB, OFB. (Ref. Stinson [20], Buchmann [3]) Breaking an Affine cipher using a known-plaintext attack. Feistel's ciphers. (Ref. Stinson [20], Landau [10]-[11]-[12])

WEEK 10.

Lecture 18 (11/29/2021). The DES (Data Encryption Standard. Comments about DES security. (Ref. Addenda [13], Stinson [20], Landau [10]-[11]-[12]). Triple DES. (Ref. Addenda [13], Stinson [20], Landau [10]-[11]-[12]). Historical news about the design of AES. Remarks on Finite Fields: F_4. (Ref. Buchmann [3]).

Lecture 19 (11/30/2021). Remarks on Finite Fields: F_{256}. AES-Rijndael128 (Advanced Encryption Standard): round descriptions, state s, functions SR, S, MC, E (Ref. Buchmann [3]).

WEEK 11.

Lecture 20 (12/06/2021). AES-Rijndael (Advanced Encryption Standard): deciphering prescriptions (Ref. Buchmann [3]). The Double Lock protocol [15]. The Vernam code: classical and modern version. Why you cannot use the Vernam code in the double lock protocol. Definition of perfect secrecy. Shannon's theorem on perfect secrecy (part 1). (Ref. Stinson [20], Buchmann [3], Smart [19])

Lecture 21 (12/07/2021). Shannon's theorem on perfect secrecy (part 2). (Ref. Stinson [20], Buchmann [3], Smart [19]) Exchange keys in three steps: The Diffie-Hellman protocol, the Diffie-Hellman problem and the Discrete Log problem. (Ref. Buchmann [3], Koblitz [9]) The ElGamal cryptosystem. Digital signature using the ElGamal cryptosystem. (Ref. Buchmann [3], Koblitz [9])

WEEK 12.

Lecture 22 (12/13/2021). Shanks' algorithm (Baby Steps, Giant Steps) for computing the discrete log in $\mathbb{Z}_p^*$. Why it is important to sort the baby-steps list; differences with Stinson's version of the Baby Steps, Giant Steps algorithm. (Ref. Stinson [20]; different version with always the worst case estimate). The B-smoothness test.

Lecture 23 (12/14/2022). The "Index-calculus" algorithm for computing the discrete log in $\mathbb{Z}_p^*$. (Ref. Pomerance [17]). Pollard's ρ method for the discrete log. (Ref. Pomerance [17]).

WEEK 13.

Lecture 24 (12/20/2021). The Chaum-van Heijst-Pfzimann compression function (based on the discrete log problem). (Ref. Koblitz [9]) Zero-knowledge proof of the Discrete Log.

References

[1] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P*, Annals of Mathematics **160** (2004), 781–793, http://annals.math.princeton.edu/wp-content/uploads/annals-v160-n2-p12.pdf.

[2] D. Boneh, *Twenty years of attacks on the RSA cryptosystem*, Notices Amer. Math. Soc. **46** (1999), 203–213.

[3] J. Buchmann, *Introduction to Cryptography*, second ed., Springer-Verlag, 2004.

[4] B.A. Cipra and P. Zorn, *Divide and Conquer*, What's happening in the mathematical sciences, vol. 3, A.M.S., Jan 1996, pp. 39–47.

[5] R. Crandall and C. Pomerance, *Prime numbers. A computational perspective*, second ed., Springer-Verlag, 2005.

[6] A. Granville, *It is easy to determine whether a given integer is prime*, Bulletin Amer. Math. Soc. **42** (2005), 3–38, http://www.ams.org/bull/2005-42-01/S0273-0979-04-01037-7/home.html.

[7] J.M. Hinek, *Cryptanalysis of RSA and its variants*, Chapman & Hall/CRC, 2009.

[8] H. Knopse, *A course in Cryptography*, American Mathematical Society, 2019.

[9] N. Koblitz, *A Course in Number Theory and Cryptography*, second ed., Springer-Verlag, 1994.

[10] S. Landau, *Communications Security for the Twenty-First Century: the Advanced Encryption Standard*, Notices of the American Mathematical Society **47** (2000), 450–459.

[11] S. Landau, *Standing the Test of Time: the Data Encryption Standard*, Notices of the American Mathematical Society **47** (2000), 341–349.

[12] S. Landau, *Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard*, Amer. Math. Monthly **111** (2004), 89–117.

[13] A. Languasco and A. Zaccagnini, *Addenda for the cryptography course*, (2015), Available on-line http://www.math.unipd.it/~languasc/corso-crittografia/Addenda-Crypto.pdf.

[14] A. Languasco and A. Zaccagnini, *Manuale di Crittografia*, Ulrico Hoepli Editore, 2015, http://www.hoepli.it/libro/manuale-di-crittografia/9788820366902.html.

[15] A. Myers, *Cs 513: System security, Lecture 05*, http://www.cs.cornell.edu/courses/cs513/2006fa/lectures/lec05.html.

[16] C. Pomerance, *A tale of two sieves*, Notices American Mathematical Society **43** (1996), 1473–1485.

[17] C. Pomerance, *Elementary thoughts on discrete logarithms*, Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography (New York) (J.P. Buhler and P. Stevenhagen, eds.), Math. Sci. Res. Inst. Pub, vol. 44, Cambridge U. P., 2008, http://math.dartmouth.edu/~carlp/PDF/dltalk4.pdf, pp. 385–396.

[18] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge U. P., 2005, https://www.shoup.net/ntb/.

[19] N. P. Smart, *Cryptography, an introduction*, McGraw-Hill, 2002, the third editon is avaliable online here: http://www.cs.bris.ac.uk/~nigel/Crypto_Book/.

[20] D. Stinson, *Cryptography: Theory and Practice*, third ed., Chapman & Hall/CRC, Boca Raton, 2006.