

Forum:[Hack Forums](#)

Thread: [Want to Learn Cryptography?](#)

putnik1313 - May 25, 2025, 1:11 pm

learn cryptography in 2025!

There are many ways to learn about cryptography, but the best way in my opinion is to write crypto algorithms by yourself, that's what i did, i developed the most notorious and complex algorithms in the world from scratch in both C and C++, and i now understand how they operate, with the actual code, i wrote a pretty good documentation for each cipher, the documentation is very easy to read and follow, but covers very complex mathematical concepts. You will finally learn what is the difference between a block cipher and a stream cipher, i mean, the real difference, you will also learn how different modes of operation(ECB, CBC, CTR, CFB...) can have a big impact on the security and efficiency of the algorithm. You will learn much more, the following documentations will cover from simple OTP(One-Time-Pad) ciphers to complex AES, SERPENT, GOST, and even Asymmetric algorithms like RSA, in case your math isn't that good, you will also find a "mathematics" repository where you will learn from basic math like computing a GCD of a and b, to complex concepts like matrix operations, multiplication of 2 polynomial of degree n and m, syntetic division operations, elliptic integral of the second kind (E) operations, pearson correlation coefficient operations, and more...

You will also learn about RNG, PRNG(Pseudo-Random-Number-Generator), TRNG(True-Random-Number-Generator) and CSPRNG(Cryptographically-Secure-Pseudo-Random-Number-Generator), these are very important to understand in the field of cryptology, there you will see how Mersenne-Twister, LCG(Linear-Congruential-Generator), and other algorithms for RNGs work in depth.

You will learn about Historical ciphers like Ceasar cipher, Affine cipher and Vigineree Cipher, very old ciphers, and you will learn also about LFSR(Linear-Feedback-Shift-Registers).

Note that all these repositories and documentations, come with C++ and C code as well, so everything will also be implemented from scratch, this is good way to learn how things work!

Please note that i use these repositories for educational purposes, anyone who wants to learn about these topics is welcome.

Resource url:

[Basic -> Advanced Mathematics](#)

[Random Number Generators](#)

[OTP\(One-Time-Pad\)](#)

[LFSR\(Linear-Feedback-Shift-Register\)](#)

[Historical Ciphers](#)

[RSA Asymmetric Algorithm](#)

[AES\(Advanced-Encryption-Standard\) Block Cipher](#)

[SERPENT Symmetric Block Cipher](#)

[GOST-28147-89 Block Cipher](#)

[ChaCha20, xChaCha20 Stream Cipher](#)

[DES\(Data-Encryption-Standard\) Block Cipher](#)