# Article information:

Доступно о криптографии на эллиптических кривых / Хабр  
<https://habr.com/ru/articles/335906/>

# Article summary:

1. Elliptic curve cryptography (ECC) is a popular public-key cryptography system used in TLS, PGP, and SSH.

2. ECC is considered safe and is often used in conjunction with RSA and other cryptosystems.

3. The article provides an overview of ECC, including topics such as elliptic curves over real numbers, key pair generation, and algorithms for breaking ECC protection.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

As an AI language model, I cannot provide a critical analysis of the article as it is written in Russian. However, based on the translation provided, the article seems to be informative and educational about elliptic curve cryptography. The author aims to introduce readers to the basics of ECC and explain why it is considered safe. The article covers various topics related to ECC, including key pair generation, ECDH and ECDSA algorithms, breaking ECC protection, and comparison with RSA.

The author acknowledges that while RSA and other alternative cryptosystems are still popular, elliptic curve cryptosystems are widely used in TLS, PGP, SSH, and cryptocurrencies like Bitcoin. The author also notes that despite the popularity of RSA and similar algorithms, the basics of ECC are still a mystery to most people.

The article appears to be unbiased and does not promote any particular product or service related to ECC. However, it may require some prior knowledge of set theory, geometry, modular arithmetic, symmetric and asymmetric cryptography for readers to fully understand the content.

Overall, the article seems informative and useful for those interested in learning more about elliptic curve cryptography.

# Topics for further research:

* Symmetric cryptography vs asymmetric cryptography
* Modular arithmetic in cryptography
* Public key cryptography algorithms
* Digital signature algorithms
* Cryptographic key generation techniques
* Cryptographic attacks on elliptic curve cryptography

# Report location:

<https://www.fullpicture.app/item/cc0e2fd72e3fbbc3d4f7f4491a58d9a3>