عنوان مقاله:

Cryptography With Maple Mathematical Software

محل انتشار:

دومین همایش ملی ریاضیات و کاربردهای آن در علوم مهندسی (سال: 1394)

تعداد صفحات اصل مقاله: 15

نویسندگان:

Davood Mosayyebi Jouybari - *MA candidate,University,Guilan,Iran*

HamidReza Nazari - *MA candidate,Hadaf University,Sari,Iran*

MirMousa Hashemian - *Member of Iranian Society of Machine Vision and Image Processing*

خلاصه مقاله:

Cryptography is the art and science of secure data communications over insecure channels. It is a very old subject, as old as our human civilization, but in the last 40 years the subject has experienced explosive growth which has led to deep changes both in its foundations and methodology, and many new applications have arisen that were not even dreamed of in the middle of the twentieth century. On the foundational side, we have seen the mergenceof key concepts, such as that of one-way function, which now occupies a central role not only in public-key cryptography, where it originated, but also in private-key cryptography. Methodologically, randomness and complexity have surged to the forefront and, with their help; security has been rigorously defined in such a way that makes it possible to obtain reductionist proofs which show that some cryptographic schemes are secure on theassumption that certain mathematical problems are computationally hard. These security reductions do not guarantee the security of a scheme in an absolute sense because, in addition to the fact that no computational problems have been proven to be hard so far. On top of all this, cryptography is currently being used by almost everyone on a daily basis when, say, connecting to a WiFi network, using a Web browser to make a secure connection, making a payment with a credit card, and so on. This has led to the development of cryptographic schemes that, besides enjoying good security properties, are sufficiently efficient for real world use. This paper, in addition to discussing the relevant theoretical constructions, employs Maple software to implement most important cryptographic schemes in use today, as well as the main cryptanalytic attacks against these schemes. And the main cryptanalytic attacks mentioned in the text. These implementations include all the relevant algorithms for example, key generation, encryption, decryption, signing, and verification. We should also warn the reader against the dangers of plain RSA. We must warn the reader that the Maple implementations of cryptographic schemes given here are not intended for standard cryptographic use . The Maple code and the programming examples try to build a bridge between the world of theoretical cryptography, and the world of practitioners. The Maple constructions given in this paper are not only limited to cryptographic schemes but also include number theoretic algorithms used in many cryptographic primitives. The use of a computer algebra package greatly facilitates the implementation of schemes and algorithms because man ...

کلمات کلیدی:

Cryptography,Cryptanalysis,Public-key,RSA,Maple

لینک ثابت مقاله در پایگاه سیویلیکا: