Cryptography Using Chebyshev Polynomials

Getting the books **cryptography using chebyshev polynomials** now is not type of inspiring means. You could not deserted going in imitation of books collection or library or borrowing from your contacts to entry them. This is an entirely easy means to specifically get guide by on-line. This online broadcast cryptography using chebyshev polynomials can be one of the options to accompany you in the manner of having new time.

It will not waste your time. admit me, the e-book will extremely circulate you supplementary business to read. Just invest tiny grow old to contact this on-line message **cryptography using chebyshev polynomials** as without difficulty as evaluation them wherever you are now.

The site itself is available in English, German, French, Italian, and Portuguese, and the catalog includes books in all languages. There's a heavy bias towards English-language works and translations, but the same is true of all the ebook download sites we've looked at here.

Cryptography Using Chebyshev Polynomials

pute Chebyshev polynomials, and that the inverse problem of com-puting the degree n, the discrete log problem for T n(x) mod p, is as difficult as that for xn mod p. 1 Introduction If Alice wants to send a secret message to Bob, using a conventional secret key cryptographic algorithm such as the DES (Data Encryption Standard)

Cryptography using Chebyshev polynomials

We consider replacing the monomial xn with the Chebyshev polynomial Tn(x) in the Diffie-Hellman and RSA cryptography

algorithms.

[PDF] Cryptography using Chebyshev polynomials | Semantic ...

CiteSeerX - Document Details (Isaac Councill, Lee Giles, Pradeep Teregowda): We consider replacing the monomial xn with the Chebyshev poly-nomial Tn(x) in the Diffie-Hellman and RSA cryptography algorithms. We show that we can generalize the binary powering algorithm to com-pute Chebyshev polynomials, and that the inverse problem of com-puting the degree n, the discrete log problem for Tn(x ...

CiteSeerX — B.: Cryptography using Chebyshev polynomials

Based on Chebyshev polynomials, you can create an asymmetric cryptosystem that allows secure communication. Such a cryptosystem uses the fact that these polynomials form a semi-group due to the composition operation. This article presents new cryptosystems that use

other than semi-group property dependencies.

The application of modified Chebyshev polynomials in ...

Then in Section 4 we propose improved scheme in client-server environment using Chebyshev polynomial in modular prime number field. In Section 5 , we analyse our proposed scheme on two aspects, namely, security and efficiency.

Improved Chebyshev Polynomials-Based Authentication Scheme ...

Encryption algorithm based on Chebyshev polynomials over finite fields Recently, a public-key encryption algorithm based on Chebyshev polynomials over prime finite fields was pro- posed [6]. In addition to the semigroup property, the pseudo-randomness of these polynomials is an attractive feature for cryptographical purposes.

Public-key encryption based on

Chebyshev polynomials over ...

Chebyshev polynomials based public key cryptosystem (CPPKC), as a kind of chaos based cryptography,,, key of CPPKC can guarantee the security even for small integer, so there is no need to look for...

Public-Key Encryption Based on Chebyshev Polynomials ...

Abstract: Chebyshev polynomials have been recently proposed for designing public-key systems. Indeed, they enjoy some nice chaotic properties, which seem to be suitable for use in Cryptography. Moreover, they satisfy a semi-group property, which makes possible implementing a trapdoor mechanism.

[cs/0411030] Security of public key cryptosystems based on ...

Cryptography using Chebyshev polynomials 2004.] 2 Optimality of Chebyshev Polynomials There's only one bullet in the gun. It's called the

Chebyshev polynomial. { Rocco Servedio via Moritz Hardt (Zen of Gradient Descent blog post). It turns out, that the optimal jump polynomials are given by the Chebyshev polynomials (of the rst kind).

Chebyshev Polynomials and Approximation Theory in ...

The Chebyshev polynomials Tn are polynomials with the largest possible leading coefficient whose absolute value on the interval [−1,1] is bounded by 1. They are also the extremal polynomials for many other properties. Chebyshev polynomials are important in approximation theory because the roots of Tn (x),...

Chebyshev polynomials - Wikipedia

Kocarev and Tasev 4 projected a PKC technique using Chebyshev polynomials define over real numbers by supplanting the multiplications in traditional procedures with the reiteration of Chebyshev polynomials characterized on

real numbers. Some favorable position is that this procedure improves the contemporary public key family and releases novel directions for research in the area of PKC.

Chebyshev chaotic map-based ID-based cryptographic model ...

Based on Chebyshev polynomials, you can create an asymmetric cryptosystem that allows secure communication. Such a cryptosystem uses the fact that these polynomials form a semi-group due to the...

Public-key encryption based on Chebyshev maps | Request PDF

More on Security of Public-Key Cryptosystems Based on Chebyshev Polynomials

(PDF) More on Security of Public-Key Cryptosystems Based ...

An N th -order interpolation function using the Chebyshev polynomials provides an accurate ap- proximation for

any N th -order polynomial with zero error. Approximating a polynomial using the Fourier series requires more terms to reach a qualitative comparable accuracy.

PROPERTIES OF CHEBYSHEV POLYNOMIALS

Chebyshev polynomials We have seen that Fourier series are excellent for interpolating (and differentiating) periodic functions defined on a regularly spaced grid. In many circumstances physical phenomena which are not periodic (in space) and occur in a limited area. This quest leads to the use of Chebyshev polynomials.

Function approximation: Fourier, Chebyshev, Lagrange

Abstract We propose public-key encryption algorithms based on Chebyshev polynomials, which are secure, practical, and can be used for both encryption and digital signature. Software implementation and properties

of the algorithms are discussed in detail.

Public-Key Encryption Based on Chebyshev Polynomials ...

The developed encryption scheme combines Chebyshev polynomial based permutation and substitution and Duffing map based substitution. A precise security analysis on the novel encryption algorithm is given.

Novel Image Encryption Scheme Based on Chebyshev ...

A recently proposed public key cryptosystem based on Chebyshev polynomials suggests a new approach to data encryption. But the security of the cryptosystem has not been investigated in depth, for lack of an appropriate analysis method.

[PDF] Parameter Selection in Public Key Cryptosystem based ...

We present a novel image encryption algorithm using Chebyshev polynomial based on permutation and substitution

and Duffing map based on substitution. Comprehensive security analysis has been performed on the designed scheme using key space analysis, visual testing, histogram analysis, information entropy calculation, correlation coefficient analysis, differential analysis, key sensitivity test, and speed test.

Novel Image Encryption Scheme Based on Chebyshev ...

Based on such polynomials, a generalization of a recently proposed public-key encryption algorithm that uses Chebyshev polynomials over prime finite fields is presented. Since our approach uses a finite field trigonometry, it is also possible to analyze some security aspects of the mentioned algorithm in the extension field scenario.