Mystery Twister 2005

International Crypto Competition

www.mystery-twister.com

Amateur, Advanced, and Expert Levels

Hans Dobbertin

Dick Gordon:

"The project is called ... SETEC ASTRONOMY."

from the movie *Sneakers* (1992)

Contents


Cryptology

The Role of Modern Cryptology for IT Security

IT Security

The world is getting smaller as a result of expanding global networks. The internet community is becoming bigger and bigger, and there are increasing opportunities for exchanging information and doing business worldwide. Home banking, e-commerce, e-government etc. offer great potential for innovation.

The internet is in principle an open medium. Nevertheless it has to be ensured that internet applications like, for instance, a digitalized financial transaction or a digitalized administrative act are legally binding and cannot be forged or manipulated.

Generally, information technology (IT) applications require security measures. Data has to be protected against loss, unauthorized access or manipulation. Countermeasures against viruses, Trojan horses, denial of service attacks etc. have to be implemented.

The realization of IT security in practice must be based on an analysis of the entire system concerned, including the environment of the IT. Once implemented, it requires continuous monitoring and supporting management.

Cryptography

Modern cryptography not only provides methods to preserve the secrecy of data by encryption, but also methods to detect manipulation of data and to prove its authenticity.

Digital signatures are a good example to illustrate the significance of cryptography. Today the requirements for legally binding digital signatures are already laid down in laws in some countries, the state Utah in the USA and Germany being among the first. It is cryptography, however, which puts the security requirements into practice.

It is quite common today for computer users to apply different kinds of cryptography: e-mail programs, such as *Pretty Good Privacy,* provide encryption and signatures, internet browsers set up secure communications, and so on.

Cryptography, implemented in the background, occurs not only in internet applications, but also if you use a smart card to store private medical information or to get money from an ATM (bank cash machine). Mobile phones authenticate themselves against the provider's base station by a cryptographic challenge-response scheme.

Designers vs. Analysts

Cryptography is concerned with the design of crypto systems, while cryptanalysis seeks to break them. These two areas are joined under the term *cryptology:*

$$\text{cryptology} = \text{cryptography} + \text{cryptanalysis}.$$

Cryptography and cryptanalysis are like two sides of the same coin. There is an intense interrelation between these two disciplines. The development of cryptology is a highly dynamic, evolutionary process.

There is a permanent fight between designers and analysts: new design ideas are targets for the analysts, and vice versa, when analysts find new attacks, the designers, for their part, must take this into account in order to avoid weaknesses. – In the context of this crypto fight, the competition Mystery Twister will offer a playful manœuvre.

The practical implementation of cryptographic schemes requires a decision, which is made very difficult as a consequence of the situation described above: one has to choose the key length and other parameters properly to ensure a sufficiently wide margin protecting against cryptanalytic attacks – the *known* cryptanalytic attacks, of course, and to some extent, also those of the future ... not an easy task, since

> "The art of prophecy is very difficult, especially about the future."
>
> Mark Twain (1835-1910)

Lack of Transparency

Most users are not aware of how strong or weak particular encryption systems are or as how reliably a digital certificate can be assessed. For many people the role of cryptography – a fundamental and very important tool for IT security – is non-transparent and sometimes even considered as being a bit magical and mystical ... or simply "cryptic".

The level of acceptance of applications like digital signatures, home banking and e-commerce is not increasing at the expected rate. There are certainly also other major causes, but not least a lack of transparency is responsible. As a result, a large part of the innovative potential of IT is not being exploited.

In view of this background we, the CITS research group (see pages 21 to 24), have taken the initiative to organize the project Mystery Twister ...

Project Mystery Twister

International Crypto Competition

Mystery Twister 2005 is an international crypto competition. During the year 2005, different tasks will be set, altogether

13 CryptoChallenges, CC1 to CC13,

of increasing difficulty, such as, for example, decrypting an encrypted message or forging a digital signature.

The variety of topics, which will be covered by the collection of challenges, is intended to provide a survey of modern cryptology.

Making Cryptology more Transparent

One of the objectives of the MYSTERY TWISTER project is to provide, in a playful way, the necessary information and insights so that non-experts can also understand what in principle is happening, usually unobserved, in the background during crypto applications.

In the past, cryptology was a secret science of the military and secret services. It was only thirty years ago that cryptology became an open science. In this relatively short period of time a large arsenal of fascinating ideas has been developed of how to encrypt and sign data, how to uncover the manipulation of data, how to exchange keys, and so on. A basic understanding of cryptographic processes and an idea of what they are capable of and where their potential weaknesses lie, is what we wish to convey through the MYSTERY TWISTER project.

Last but not least, we are organizing the competition, and it is worth participating because ...

... it is fun to break codes and uncover secrets.

Challenges Closely Related to IT in Practice

The first CryptoChallenges refer to classical manual encryption, of which the Caesar cipher is the best known example. Apart from these few exceptions, the remaining CryptoChallenges involve breaking specifically described digital cryptographic schemes. They are taken from components of IT applications occurring in practice like

- access control via password,
- authentication by a SIM card in mobile phones,
- encryption and signing of data.

The basic cryptographic concept of the original standards will not be changed, but certain weaknesses are implanted such as shortened keys or an incorrect choice of parameters.

CC13 plays a special role. It sets the task of breaking a crypto scheme with a key length in a range that is presently considered to be secure.

The chosen scheme is of fundamental importance for internet security. But at this stage we will not disclose which crypto system is concerned. It will be published in January 2005 with the start of Mystery Twister 2005.

We do not expect anybody to solve CC13. On the other hand, ... we can quote Mark Twain once again (see page 5).

Amateur, Advanced, and Expert Levels

CC1 to CC4 will be designed in such a way that no special knowledge is required. Here in Level I we address amateurs, or in other words, everyone who likes puzzles. The home page of the Mystery Twister competition (see page 15) provides a *Knowledge Base,* with comprehensive information about cryptology, especially direct suggestions and aids for the CryptoChallenges.

Level I requires no programming skills. Tools for a frequency analysis of symbols, occurring in a given encrypted text, and for similar purposes are provided in animated form on the competition home page.

Success at Level I is a good basis for participating in the advanced Level II (CC5 – CC8). The CryptoChallenges of Level II can be solved with varying degrees of effort within the time allowed, basic expertise provided, which can also be found in the Knowledge Base on the Mystery Twister website.

Level III (CC9 – CC13) of the competition addresses the leading experts worldwide and is designed to stretch the limit of what is estimated to be breakable, given the current state of the art in cryptanalysis. And with CC13, the most difficult challenge of all, we even go beyond this limit. Solving this problem would presume a major advance in cryptanalysis.

Level I (amateur): CC1 to CC4,

Level II (advanced): CC5 to CC8,

Level III (experts): CC9 to CC13.

Schedule

The time between the announcement and the latest possible submission of a solution is

1 month for each CRYPTOCHALLENGE in Level I (consecutively),

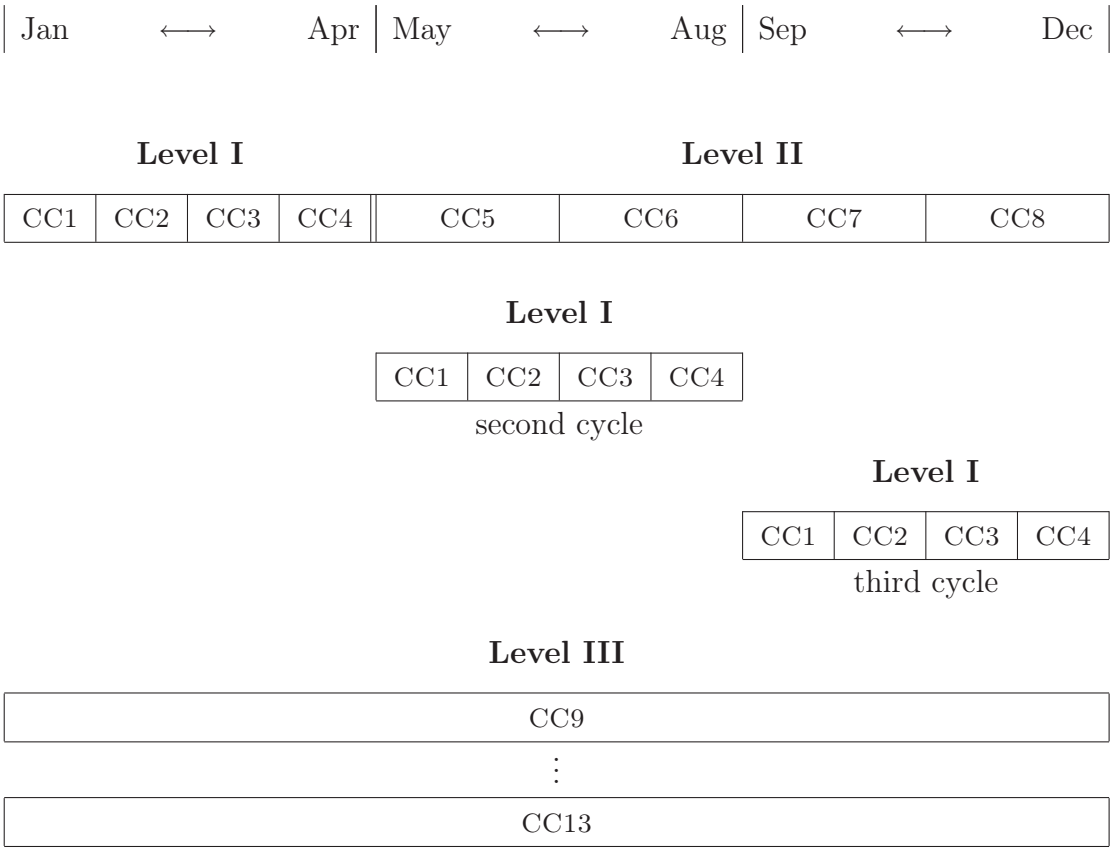
2 months for each CRYPTOCHALLENGE in Level II (consecutively),

1 year for all CRYPTOCHALLENGEs in Level III (parallel).

Level II will take place subsequent to Level I, and Level III will run during the entire year 2005. Two further cycles of Level I with new variations of the previously set tasks are envisaged for late entries.

The CRYPTOCHALLENGEs CC1 to CC8 of Level I + II will be made available after each other, whereas CC9 to CC13 of Level III will be made available at the same time (see next page).

Calendar for Mystery Twister in 2005



Prizes

There are prizes to be won for each CRYPTOCHALLENGE. Since many correct solutions are expected at Level I, winners will have to be selected by lot. The prizes envisaged include presents, vouchers and subscriptions for IT periodicals.

At Level II, fewer participants are to be expected. The prizes proposed for this level are special software licences, hardware items like hand-held computers or visits to research facilities.

The first person to submit a correct solution of a CRYPTOCHALLENGE from Level II will be the prize winner. Possibly, further prizes will be decided by lot.

At Level III, the expert level, money prizes will be awarded. The first person or group to submit the correct solution to a CRYPTOCHALLENGE will be the winner.

Home Page

We hope to have succeeded in arousing your interest in Mystery Twister. On the home page of the competition

`www.mystery-twister.com`

you will find further information on Mystery Twister by the end of 2004, especially a preliminary version of our Knowledge Base, the rules for submitting solutions via the internet and, once the competition has begun in January 2005, the released CryptoChallenges.

We are working intensively on our website. In October 2004 various material will be made available, such as demo versions of CC1 and CC2. Certain areas will be reserved for special visitors and will therefore be password-protected. In order to receive access or if you have any questions or comments, please e-mail the following address:

`mystery@cits.rub.de`


CeBIT
Press

Publicity

In general, there is great public interest in cryptology. This is why we expect to achieve considerable publicity in the press, on TV and on the internet now that the planned competition has taken shape and major preparations have been completed. Although, at this stage there is no reliable basis yet for estimating the number of participants that can be expected.

We started a first publicity campaign in spring 2004. On our stand at the CeBIT 2004 exhibition in Hanover (Germany) we presented an animated CryptoChallenge of Level I, which was received with great interest. The demonstration of Mystery Twister at the exhibition was reported in daily newspapers and on the Heise News Ticker.

We are in touch with various popular scientific and computer magazines as well as with several newspapers which are planning to publish articles about our competition. A TV science program has shown interest in featuring a report. We are currently discussing the prospect of a book to accompany the competition with the scientific publishing company Springer (Berlin, Heidelberg, New York)

Together with the press office of the Ruhr-University Bochum, we are planning to launch a campaign at the start of the competition, addressed mainly at the scientific press and at universities.

Partners and Sponsors

The idea of organizing a crypto competition was first suggested to us by *SecWare Technologies AG,* `www.secware.de`, who market crypto products.

We wish to thank the group of designers and programmers at *Gainware,* `www.gainware.de`, for their help in the first stage of designing the MYSTERY TWISTER website.

The companies

Sun Microsystems, `www.sun.de`,

CADAC, `www.cadac.de`,

are already sponsors of the MYSTERY TWISTER project ...

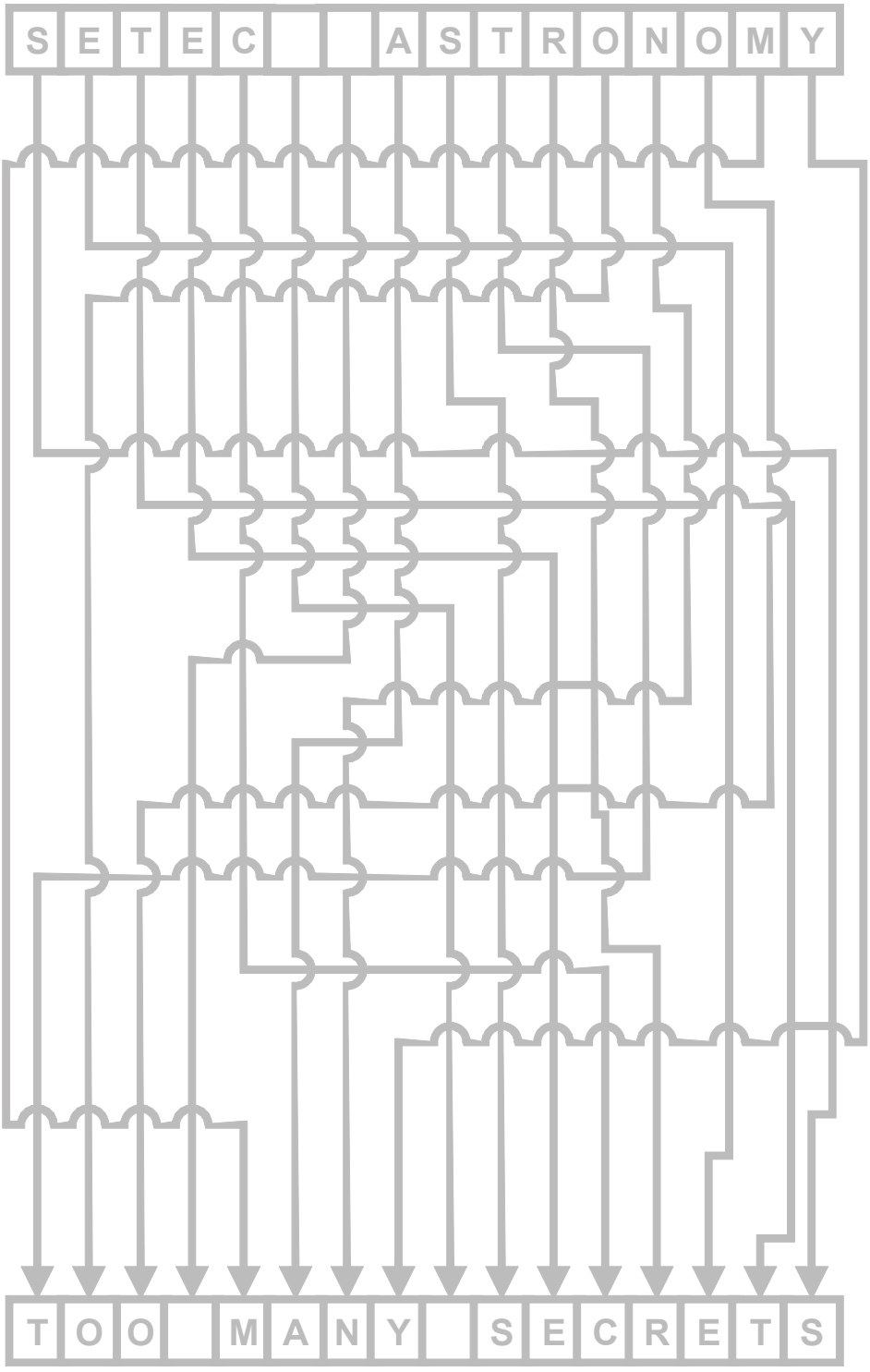
Sponsors Wanted

... we are still looking for sponsors to enable us to continue designing our CryptoChallenges and their internet presentation at a high level and to fund prizes for the solution of the tasks concerned. Sponsored gifts to be awarded as prizes are, of course, also welcome.

In order to promote your company or institution and to highlight your support of the competition, we would, of course, name and link you as a sponsor on the Mystery Twister website. Our sponsors are also mentioned in our competition publicity activities.

We can think of many ways to cooperate with sponsoring (and non-sponsoring) partners. Should you therefore consider supporting our Mystery Twister project, you can contact us by phone or by e-mail:

Hans Dobbertin
phone: +49 (0)234 32 23 261
e-mail: hans.dobbertin@ruhr-uni-bochum.de


SETEC ASTRONOMY
TOO MANY SECRETS

About Us

We, the CITS Research Group, ...

... are organizing and presently preparing the competition Mystery Twister.

Since October 2001, Hans Dobbertin holds the newly founded chair for Cryptology and IT Security (CITS) in the Faculty of Mathematics at the Ruhr-University Bochum. (Bochum is a city in the Ruhr region of Germany, close to Cologne. The Ruhr-University Bochum, founded in 1962, presently has about 29,000 students.)

The CITS research group works on both foundations and practical applications of cryptology. Main topics are for instance

> block ciphers, stream ciphers, hash functions, multi-variate asymmetric schemes, elliptic and hyper-elliptic curves, side channel attacks.

An important crypto event this year, AES4, the Fourth Conference on the Advanced Encryption Standard (May 10 – 12, 2004, Bonn, Germany) was an initiative of the CITS group. AES4, `www.aes4.org`, was organized by A. Sowa (general chair), H. Dobbertin (program chair), and V. Rijmen (program chair) from the Graz University of Technology.

CITS is Co-founder of the Horst Görtz Institute

The CITS group is integrated into a competence center for IT security, which has been established in Bochum over the last years.

In 2002 the Horst Görtz Institute (HGI), `www.ruhr-uni-bochum.de/hgi`, was founded at the Ruhr-University of Bochum by CITS and the research groups

Communication Security (COSY),

Net and Data Security (NDS).

These two groups are part of the Faculty of Electronics and Information Technology.

ISEB, an institute focusing on security in e-business, within the Faculty of Economics, is also integrated in the HGI. An expansion of the HGI in order to also cover legal and social aspects of IT security is planned in the near future.

The HGI is named after Dr.-Ing. h.c. Horst Görtz, founder of *Utimaco Software AG,* whose generous sponsorship made it possible to build up this institute.

Diploma, Master's, and Ph.D. Programs in IT security are offered by the HGI and its associated faculties.

In 2003 *eurobits* (`www.eurobits.de`) was founded, a union of HGI with several companies located close to the university campus, whose business is education, development and consulting in the field of IT security.

CITS is Partner in ECRYPT

The CITS and COSY research groups of the Horst Görtz Institute (see previous page) participate in the project

ECRYPT (European Network of Excellence for Cryptology),

which is funded within the European Commission's Sixth Framework Programme (see `www.ecrypt.eu.org`).

The main objective of ECRYPT is to ensure a durable integration of European research in cryptology and to maintain and strengthen the European excellence in these area. The 32 partners in ECRYPT are leading players in cryptology from academia and industry.

Mystery Twister Team

Scientific Staff

Hans Dobbertin, Dr., full professor
Tanja Lange, Dr., post-doc assistant
Magnus Daum, Dipl.-Math.
Patrick Felke, Dipl.-Math.
Gregor Leander, Dipl.-Math.

Technical Support

Elena Prokhorenko, Dipl.-Phys.

Public Relations

Aleksandra Sowa, Dipl.-Volksw.

Home Page Design

Thorsten Doliwa, student
Benedikt Gierlichs, student
Michael Kallweit, student
Bouchta Lakhal student
Maxim Zaks, student

Contact

Hans Dobbertin
phone: +49 (0)234 32 23 261
fax: +49 (0)234 32 14 430
e-mail: hans.dobbertin@ruhr-uni-bochum.de

CITS Research Group
Faculty of Mathematics
Ruhr-University Bochum
URL: www.ruhr-uni-bochum.de/cits

MYSTERY TWISTER 2005 (www.mystery-twister.com) is an international crypto competition organized by the

Cryptology and IT Security (CITS)
Research Group
www.ruhr-uni-bochum.de/cits

of the Ruhr-University Bochum. As the name suggests, it will take place during the year 2005.

Thirteen CRYPTOCHALLENGEs of increasing difficulty at amateur, advanced, and expert levels will be set.

In the first and second part of this booklet you can find information about the background, aims, scope, and schedule of the competition. A short portrait of the CITS research group and its activities is added in the third part.