The CrypTool Project – Improving Awareness and Education for Cryptology

a report by
Bernhard Esslinger

Head, Global Competence Center for Cryptography, PKI and IT Security Technology Research Department, Deutsche Bank

The ever-increasing complexity of information technology (IT) systems and applications significantly increases the demand for additional IT security mechanisms and technologies. However, implementing security technology is only one side of the coin. Even more important is creating a general awareness of IT security issues based on a broad understanding of the underlying concepts.

IT Security and Cryptology

A key enabler of IT security is the broad area of cryptology. Cryptology itself is an umbrella term for cryptography (primarily concerned with encryption and authentication methods) and cryptanalysis (the analysis and evaluation of cryptographic methods). Cryptography provides methods to achieve the fundamental IT security protection goals of authentication, confidentiality, integrity and non-repudiation.

Cryptographic methods and algorithms are implemented in nearly all forms of electronic communication, including cell phones, cash machines, online banking, e-commerce, secure email, digital tickets or rights management for digital contents, just to name a few. Although cryptography is already a part of our everyday life (including ignition lock-out systems, mobile phones and pay TV), the perceived complexity of cryptology is often a major barrier in gaining a better understanding of the basic mechanisms. However, a basic understanding of cryptology is definitely required to establish an effective awareness of IT security issues.

Raising Awareness through Education using CrypTool

In 1998, Deutsche Bank launched a project called CrypTool in order to further improve the education of its personnel, specifically in terms of IT security and cryptography. Over the years, CrypTool has been further developed as an open-source project in a close and successful co-operation between Deutsche Bank and several universities. Even though it was initially intended for the bank's internal use only (in order to educate and train apprentices, as well as IT personnel), the bank soon decided to publish CrypTool as free software for the Internet community. By sharing its experiences and best practice in IT security, the project has greatly benefited from global user feedback and the involvement of additional developers.

The objective of CrypTool is not only to provide a tool for IT experts within the financial services industry, where a deeper understanding of available cryptology mechanisms as well as potential attacks is essential; it is also to offer a more general cryptology education tool that visualises the use of a broad set of cryptology concepts and methods from ancient to state-of-the-art encryption algorithms implemented in modern electronic communication. In this respect, CrypTool has also benefited from the close co-operation with universities ensuring the academic correctness of the implementation.

As of today, CrypTool is being hosted by the Technical University of Darmstadt and is globally used as an e-learning tool by leading universities, companies and agencies to educate students and employees in cryptography and IT security.

CrypTool as an e-Learning Application

CrypTool combines two important aspects: being an e-learning application that supports 'playful learning' on the one hand; and, on the other, acting as a professional tool, in the sense that it is mathematically and cryptographically correct and reflects the current state of technology. Hence, CrypTool can be used to visualise the basic concepts of cryptology (including digital signatures, symmetric, asymmetric and hybrid encryption, protocols, etc.) and it can be utilised by IT experts in order to evaluate certain algorithms and test specific settings.

CrypTool features a comprehensive collection of cryptographic algorithms that are not only implemented but also documented in detail, explaining the algorithms, as well as potential attacks, and to build a better understanding of the advantages and disadvantages related to specific algorithms.

Bernhard Esslinger joined Deutsche Bank in 1998 as global head of IT security, in charge of activities like the global introduction of Information Security Policies and Standards, the global employee awareness programme, the development of the Deutsche Bank security strategy and the set-up of global security infrastructure projects. He co-ordinated and realised the PKI infrastructure of Deutsche Bank and delivered top management support for issues like public-private partnership and digital signatures (acting as Deutsche Bank's delegate in the German Signature Alliance). Currently, he acts as head of the global competence center for cryptography and as head of the IT security technology research department. Before joining Deutsche Bank, he worked for 10 years in various positions at SAP, such as Chief Security Officer of SAP world-wide. Bernhard Esslinger is a speaker at various international conferences and serves as a lecturer at the Business Information Systems Institute at the University of Siegen, Germany. He is also one of the founders of the European Bridge-CA (www.bridge-ca.org) and initiator and head of the Internet development project CrypTool, delivering an open source e-learning program about cryptography and IT security awareness (www.cryptool.org).

Table 1: IT Security Protection Goals and Corresponding Cryptography Methods

Protection goal	Description	Cryptography methods
Authentication	Authentication ensures that users are identified and that these identities are appropriately verified.	Digital signature, message authentication code (MAC), challenge response
Confidentiality	The stored or transferred information is not disclosed to unauthorised individuals, entities or processes.	Encryption
Integrity	Integrity ensures that data has not been altered or destroyed in an unauthorised manner.	Digital signature, MAC, hash function
Non-repudiation	The principle that, afterwards, it can be proven that the participants of a transaction did really authorise the transaction and that they have no means to deny their participation.	Digital signature

CrypTool Facts

- Website: www.cryptool.org
- Current version: 1.4.00 (the complete version of CrypTool is available in English and German)
- Origin: started in 1998 as awareness initiative and co-operation project between Deutsche Bank AG and universities
- Status: active open-source project with currently more than 30 developers globally – further contributors are warmly welcome!
- Main sponsor: Deutsche Bank
- Hosting: Technical University of Darmstadt
- Awards: e.g. TeleTrusT Special Award, and a finalist in the European Information Security Award (2004), given at the conference 'RSA-Europe'
- Usage: awareness and education for companies and universities, with more than 2,000 downloads per month

A typical real-life example of applied cryptography is the digital signature. A broad implementation of the digital signature as a means for authentication, integrity and non-repudiation would be highly beneficial, not only from an economic but also from a security point of view, saving trips to authorities or banks for any individual and providing secure documents in parallel. Nearly everyone has heard the term digital signature, but for the majority (and this includes some IT specialists as well) it still remains a mystery. How does it actually work, how does it protect the integrity of the document, how can it be validated and how secure is it?

CrypTool visualises the concept of digital signatures using an interactive data flow diagram and explains potential attacks using modern algorithms. The user can walk through the generation and validation of the digital signature in a step-by-step approach.

Similar to the digital signature, the concepts of encrypted connections to servers using standards such as HTTPS/SSL, or the S/MIME standard for encrypted email are also often only vaguely understood. Even though terms and technology themselves are frequently used in everyday life, awareness and education for those technologies are often very limited. Thus, for example, only a few security-aware users look for the key lock icon in a Web browser when accessing a website containing sensitive information. Additionally, even using an encrypted connection does not necessarily mean that the information is actually transferred to the appropriate receiver; this highlights the very important fact that encryption without authentication does not provide appropriate IT security.

Inadequate authentication is one reason why current phishing attacks succeed. Other reasons are that it is very easy to fake an email's origin. This could be avoided easily by using digital signatures on emails – a mechanism all standard email clients (like Outlook or Thunderbird) already support from a technical point of view. In addition, this would require building a trusted certificate infrastructure.

Many organisations, such as Boeing, Chevron, Microsoft, SAP, Deutsche Bank, UBS, Bosch,

German Federal Bank or Siemens, already have a cost-effective internal public key infrastructure (PKI). If these companies participate further in bridging organisations like the European Bridge-CA (www.bridge-ca.org), then we could reach a broad trust in email certificates.

In this respect, CrypTool graphically explains how authentication within a client server environment and hybrid encryption actually works. An interactive demonstration allows the user to test different authentication methods and also highlights potential opportunities for attackers, providing in-depth knowledge about the weaknesses of a given authentication method.

Last but not least, CrypTool supports cryptanalysis. The tool features a broad set of methods to analyse encrypted data sets, such as analysis for floating frequency, autocorrelation, entropy, compressibility, n-gram-analysis, random analysis with three-dimensional (3-D) visualisation, brute force and side-channel attacks. This collection of powerful features enables a security specialist to analyse and evaluate existing applications to further improve a company's IT security. This way, a security specialst can gain a clear understanding which algorithms, combined with which key length, can be considered secure. It will also improve awareness of the fact that it is not single algorithms alone, but the intelligent combination of the cryptographic basic mechanisms in protocols and products (like file server encryption) that create security.

Knowledge about the weaknesses in products and an understanding of the specific requirements of one's own business are necessary to select the appropriate products for one's own organisation.

Conclusion and Outlook

The increasing complexity of IT systems leads to new challenges in IT security. Cryptology is and will always be an essential part of IT security, and its concepts and methods remain fundamental. Cryptology education is required more than ever to not only raise awareness but also to influence further IT developments towards more secure and effective IT solutions.

The experiences of the Deutsche Bank CrypTool project shows how IT security awareness can be successfully raised through improved education. As an open-source project, the tool can be utilised without licences in other companies, agencies or universities in order to raise the awareness for IT security issues and the appropriate implementation of cryptology. ■

Figure 2: Cryptology Can Be an Effective Enabler by Providing Awareness and Technology for IT Security

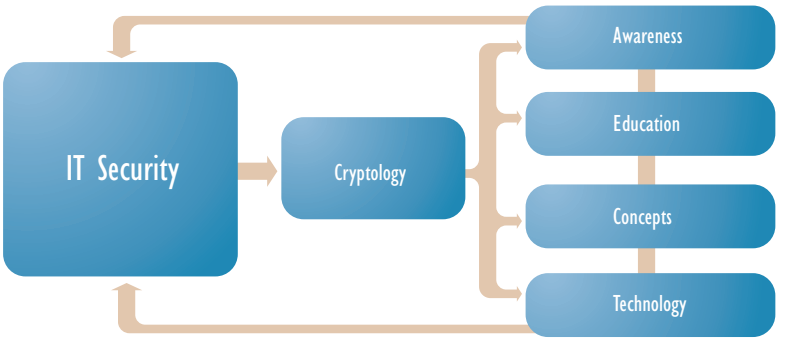

Figure 3: Interactive Generation of a Digital Signature in CrypTool

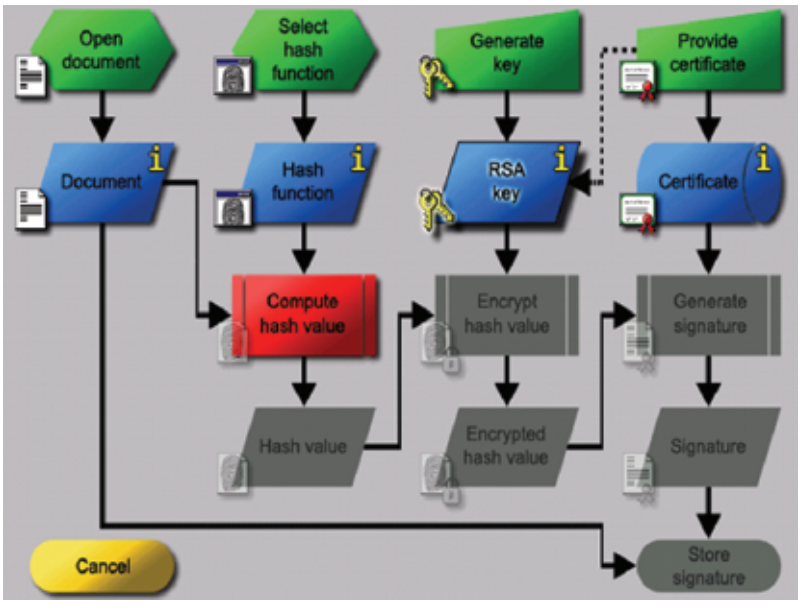

Figure 4: Interactive Demo About Different Authentication Mechanisms