# Understanding encryption

An overview of the history and evolution of cryptographic algorithms and decryption

digicert®

# Table of contents

digicert®

# Introduction

Ciphers have been in use since 3000 B.C., but their importance and relevance for information security has increased with the growth of the Internet and the escalating volumes of data exchanged online every day.

The history of ciphers and encryption is a compelling one – being a constant battle between encryption by cryptographers and decryption by cryptanalysts, with repeated cycles of development of a cryptographic algorithm, attempts to break it, followed by the development of a new cipher algorithm.

This paper examines the history of ciphers and the associated breakthroughs in technologies, along with a number of measures that users of modern ciphers should deploy.

# How it all began

The oldest-known ciphers are said to be hieroglyphics (ancient Egyptian script) on monuments dating back to around 3000 B.C., which were considered undecipherable until the 19th century. Due to so few people being taught to read them, this can be considered a form of cryptography.

However, around the sixth century B.C., the Scytale cipher was used in the ancient Greek city-state of Sparta. Employing this cryptography, messages were written on a strip of parchment wrapped around a thick baton (a 'scytale'; see Figure 1). The strip could then only be read if the recipient possessed a baton of the same width.

**Ciphers like this – that change the order of letters – are known as 'transposition ciphers'.**

Figure 1

Next, the first century B.C. saw the emergence of the Caesar cipher, which was frequently used by the Roman Emperor Julius Caesar and is one of the most famous methods of cryptography. The cipher worked by substituting each letter in the original message for another letter located in a fixed number of positions down the alphabet, which was only known by the sender and receiver.

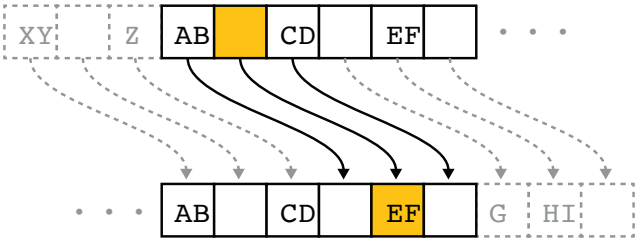


Figure 2

**Ciphers like this – that shift letters along the alphabet – are known as 'shift ciphers'.**

As these ciphers can be easily decrypted by trying out a maximum of 26 shift numbers, using a random permutation can vastly increase the number of permutations (to 26 x 25 x 24 x .... = 40000000000000000000000000!), rendering decryption far more difficult.

| | |
|---|---|
| Plain text (non-encrypted text) | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| Encrypted text | SMKRATNGQJUDZLPVYOCWIBXFEH |

An encryption method that rearranges the sequence of characters based on a fixed rule, such as that shown above, is called a 'substitution cipher'. These are the most commonly used cryptography systems throughout history, and include the modern Enigma mechanical cipher machine. (described in more depth below.)

However, substitution ciphers, including the simpler Caesar cipher, can all be decrypted using frequency analysis. This uses linguistic parameters to guess pre-encrypted letters based on how often they appear. For example, in the English language:

- 'e' is the most frequently used letter (see Figure 3)
- 'q' is always followed by a 'u'.
- Such words as 'any', 'and', 'the', 'are', 'of', 'if', 'is', 'it' and 'in' appear with high frequency.

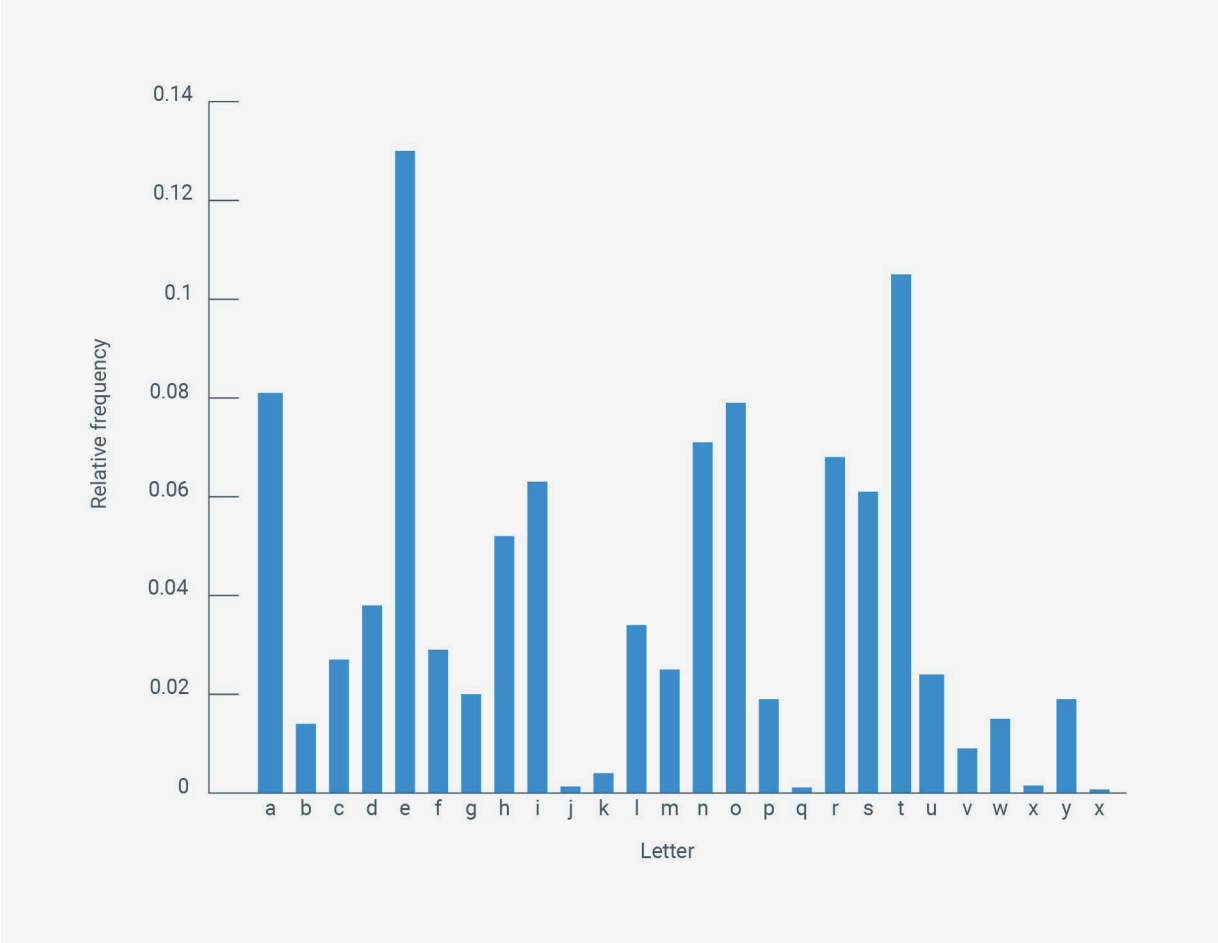


Figure 3

digicert®

# A renaissance in cryptology

During the Middle Ages diplomatic activities greatly intensified and cryptographic technologies advanced significantly, as classic ciphers were decrypted and new ciphers were invented to protect an increasing volume of confidential information.

## The Mary Queen of Scots cipher

The cipher used between Mary Queen of Scots and her other conspirators in the 16th century is known as a 'nomenclature cipher'. As well as replacing alphabetic letters, it incorporated a code for the replacement of phrases with symbols, based on a shared codebook. However, the weakness of the cipher's one-to-one assignment of encrypted letters to plaintext letters was exploited to decrypt it, which led to Mary being found guilty of treason and executed at Fotheringay Castle for plotting the assassination of Queen Elizabeth I of England.

| | |
|---|---|
| Plain text | GOLDMEDALIST |
| Key | OLYMPICOLYMP |
| Encrypted message | UZJPBMFOWGEI |

## The Vigenère cipher

During the 15th century, to overcome the inherent weaknesses of substitution ciphers or the need to share a sizeable codebook, Leon Battista Bellaso developed a prototype for a polyalphabetic substitution cipher, using multiple substitution alphabets. This paved the way for successive developments, including the final form later attributed to Blaise de Vigenère: the powerful 'Vigenère cipher'.

The Vigenère cipher cryptography uses a grid, called a Vigenère square (see Figure 4), which encrypts the plaintext e.g. 'GOLD MEDALIST', using another word e.g. 'OLYMPIC', as a key. So even if the conversion grid falls into someone else's hands, decryption is extremely difficult if the key is unknown.

| | AB | CD | EF | GH | IJ | KL | MN | OP | QR | ST | UV | WX | YZ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A** | AB | CD | EF | GH | IJ | KL | MN | OP | QR | ST | UV | WX | YZ |
| **B** | BC | DE | FG | HI | JK | LM | NO | PQ | RS | TU | VW | XY | ZA |
| **C** | CD | EF | GH | IJ | KL | MN | OP | QR | ST | UV | WX | YZ | AB |
| **D** | DE | FG | HI | JK | LM | NO | PQ | RS | TU | VW | XY | ZA | BC |
| **E** | EF | GH | IJ | KL | MN | OP | QR | ST | UV | WX | YZ | AB | CD |
| **F** | FG | HI | JK | LM | NO | PQ | RS | TU | VW | XY | ZA | BC | DE |
| **G** | GH | IJ | KL | MN | OP | QR | ST | UV | WX | YZ | AB | CD | EF |
| **H** | HI | JK | LM | NO | PQ | RS | TU | VW | XY | ZA | BC | DE | FG |
| **I** | IJ | KL | MN | OP | QR | ST | UV | WX | YZ | AB | CD | EF | GH |
| **J** | JK | LM | NO | PQ | RS | TU | VW | XY | ZA | BC | DE | FG | HI |
| **K** | KL | MN | OP | QR | ST | UV | WX | YZ | AB | CD | EF | GH | IJ |
| **L** | LM | NO | PQ | RS | TU | VW | XY | ZA | BC | DE | FG | HI | JK |
| **M** | MN | OP | QR | ST | UV | WX | YZ | AB | CD | EF | GH | IJ | KL |
| **N** | NO | PQ | RS | TU | VW | XY | ZA | BC | DE | FG | HI | JK | LM |
| **O** | OP | QR | ST | UV | WX | YZ | AB | CD | EF | GH | IJ | KL | MN |
| **P** | PQ | RS | TU | VW | XY | ZA | BC | DE | FG | HI | JK | LM | NO |
| **Q** | QR | ST | UV | WX | YZ | AB | CD | EF | GH | IJ | KL | MN | OP |
| **R** | RS | TU | VW | XY | ZA | BC | DE | FG | HI | JK | LM | NO | PQ |
| **S** | ST | UV | WX | YZ | AB | CD | EF | GH | IJ | KL | MN | OP | QR |
| **T** | TU | VW | XY | ZA | BC | DE | FG | HI | JK | LM | NO | PQ | RS |
| **U** | UV | WX | YZ | AB | CD | EF | GH | IJ | KL | MN | OP | QR | ST |
| **V** | VW | XY | ZA | BC | DE | FG | HI | JK | LM | NO | PQ | RS | TU |
| **W** | WX | YZ | AB | CD | EF | GH | IJ | KL | MN | OP | QR | ST | UV |
| **X** | XY | ZA | BC | DE | FG | HI | JK | LM | NO | PQ | RS | TU | VW |
| **Y** | YZ | AB | CD | EF | GH | IJ | KL | MN | OP | QR | ST | UV | WX |
| **Z** | ZA | BC | DE | FG | HI | JK | LM | NO | PQ | RS | TU | VW | XY |

Figure 4

## The Uesugi cipher

A similar cipher using a conversion grid was also created in Japan during the 16th century. Usami Sadayuki, military advisor of feudal warlord Uesugi Kenshin, is credited with making an encryption table based on a Polybius square, or 'checkerboard'. As the traditional Japanese Iroha alphabet has 48 letters, the grid is formed of 7 x 7 squares, with each symbol represented by the number of a row and column (see Figure 5).

| 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
|---|---|---|---|---|---|---|---|
| we | a | ya | ra | yo | chi | i | 1 |
| hi | sa | ma | mu | ta | ri | ro | 2 |
| mo | ki | ke | u | re | nu | ha | 3 |
| se | yu | fu | wi | so | ru | ni | 4 |
| su | me | ko | no | tsu | wo | ho | 5 |
| n | mi | e | o | ne | wa | he | 6 |
| | shi | te | ku | na | ka | to | 7 |

Figure 5

# Waging war on ciphers

The development of modern communications precipitated a surge in cryptography and cryptanalysis during the First World War.

## Breaking German communications

At the start of the war in 1914, when Britain declared war on Germany it cut the German's offshore submarine communication cable, so its military could only send information overseas through international cable line via Britain or by radio transmission. All subsequent intercepted communications were sent to a specialist cryptography unit at the British Admiralty, known as Room 40, for deciphering.

## The Zimmermann telegram

The Foreign Secretary of the German Empire, Arthur Zimmermann, had formulated a plan to prevent the United States of America (USA) from joining the Allies in the First World War, by enticing Mexico and Japan to attack the USA. A telegram with instructions disclosing his plans to the German Ambassador in Mexico was decrypted by Room 40. However, Britain did not initially publicise the message as it wanted to avoid Germany developing a new and more powerful cipher. Only when it obtained a plaintext version of the telegram was its existence made public, which then provoked the USA's declaration of war on Germany.

## ADFGVX cipher

In 1918, the ADFGX cipher, designed by Colonel Fritz Nebel of the German army, came into practical use. Like the Uesugi cipher, it used a Polybius square with the five letters ADFGX heading the rows and columns. Each letter in the grid corresponded to two encrypted

letters. However, a transposition cipher was then applied to the resulting series of letters for encryption. The ADFGX cipher was superseded by the ADFGVX cipher, which had been upgraded to six rows and columns (see Figure 6).

| | A | D | F | G | V | X |
|---|---|---|---|---|---|---|
| A | d | h | x | m | u | 4 |
| D | p | 3 | j | 6 | a | o |
| F | i | b | z | v | 9 | w |
| G | 1 | n | 7 | 0 | q | k |
| V | f | s | l | y | c | 8 |
| X | t | r | 5 | e | 2 | g |

Figure 6

It is practically impossible to decrypt the cipher using this grid, if the key is treated as disposable. However, this would require the sharing of a large number of keys, which would be impractical in a front-line combat situation.

## The Enigma era

The decryption of even the most complex ciphers was facilitated enormously by the advent of mechanical cipher machines from the beginning of the 20th century.

Enigma is a family of portable and secure mechanical cipher machines invented by German engineer Arthur Scherbius in 1918. As the German army was unaware that its First World War cipher had been decrypted, it had little desire to pay for an expensive upgrade to its cryptography, so it chose not to adopt Enigma technology. However, when it realised that it had lost the war largely because of British decryption of its ciphers it resolved to embrace Enigma.

Enigma's cryptography featured polyalphabetic substitution encryption. The unit was made up of multiple rotors, embedded with the 26 letters of the alphabet, known as a scrambler, and a plugboard, which carried out single alphabetic character conversions. For each letter input on the keyboard, the scrambler rotated one gradation, which enabled easy encryption or decryption, using a key that changed with each input letter.

Under threat of invasion by Germany, Poland invented an encryption machine known as Bombe, but improvements made to Enigma created an increasing number of encryption patterns, so it was uneconomical for Poland to continue its cryptanalysis work. Instead, in 1939, two weeks before the start of the Second World War, Poland passed on its research findings and decryption work to Britain. With this information Britain was able to decrypt the German army's pattern for Enigma, which meant the Enigma code was finally broken.

German information gained from the decryption of Enigma, known as Ultra, remained an important data source for the Allies until the end of the war. However, this break-through remained highly confidential, so Germany continued to use Enigma with complete faith until the end of the war. The fact that Enigma had been decrypted was not publicly disclosed until 1974.

# Entering the computer age

Since the Second World War, encryption and decryption has shifted from machine to computer. The rapid spread of computers in the private sector has also placed more importance on cryptography for corporate commercial transactions and other civilian uses, as well as military applications.

## The DES cipher

In 1973 the United States Commerce Department's National Bureau of Standards (NBS), later called the National Institute of Standards and Technology (NIST), sought proposals for a cryptography system for standard use, which publicly disclosed the cipher algorithm. In 1976, the NBS approved the Data Encryption Standard (DES) cipher, which subsequently became the worldwide standard cipher.

This was a turning point in the history of cryptography and especially the civilian applications of ciphers, as it offered a cost-effective and practical way for businesses to encrypt and decrypt sensitive information using symmetric-key cryptography – much like the Caesar cipher had done.

## Public-key cryptography

The advent of public-key cryptography finally solved the one problem that the Caesar cipher had not - how to hand over the key. Launched in 1976, by Bailey Whitfield Diffie, Martin Hellman and Ralph Merkle, public-key cryptography facilitates encrypted communications, without the need for advance delivery of keys, using a public key that anyone can access for encryption and a private key known only to the recipient for decryption.

The Diffie-Hellman-Merkle key exchange concept uses a one-way function, called modular arithmetic, which makes it possible to establish confidentiality during a conversation in a public place. This revolutionary invention significantly rewrote one of the governing principles of cryptography – that key exchange had to take place covertly.

However, at that time, what had not yet been developed was a one-way function that allows an asymmetric cipher using different keys for encryption and decryption. The development that took the theory of public-key cryptography up to the point of implementation was the RSA cipher.

## The RSA Cipher

The mathematical method to realise the Diffie-Hellman public-key concept was developed by three researchers at the Massachusetts Institute of Technology: Ronald L. Rivest, Adi Shamir and Leonard M. Adleman. Its name, RSA cipher, came from the initial letters of the three researchers' surnames.

A British cryptographer had, in fact, developed a public-key cryptography algorithm prior to the launch of the RSA cipher, but such new ciphers were treated as national secrets, so it remained a UK classified project until 1997.

The methodology employed by the RSA cipher involves factorisation of a given number into prime numbers, used as the public key and part of the private key, as in this example:

**95=5 × 19**

**851=23 × 37**

**176653=241 × 733**

**9831779=2011 × 4889**

The characteristics of such prime factorisation render it extremely difficult to read the private key from the public-key within a realistic timeframe, even if the public key is easily accessible, so it enables key exchange for decryption only by the intended party on the Internet.

For example, Transport Layer Security and Secure Sockets Layer (TLS/SSL) is a protocol for secure communications between web server and client that was introduced by Netscape Communications and embedded in Netscape Navigator. TLS/SSL is characterised by issuance of an electronic certificate that explicitly verifies the identity of the server (web server, mail server). After that, any interception, leakage or other security breaches of information passed over the Internet are prevented through encryption of messages using a symmetric key, which is safely conveyed by public-key cryptography.

## Alternatives to RSA

1. **Digital Signature Algorithm**
   DSA (Digital Signature Algorithm) is a United States. government-approved and certified encryption algorithm that was developed by the National Security Agency in 1991 as an alternative to the current standard RSA algorithm. It offers the same level of security and performance as RSA, but uses a different mathematical algorithm for signing and encryption. A DSA key pair will be the same size as the equivalent RSA key. The DSA algorithm provides the same level of security and performance as the RSA algorithm but uses a different, less commonly used mathematical algorithm. Although key sizes are identical to RSA, key generation and digital signature using DSA is faster. The tradeoff is that key verification is slightly slower.

2. **Elliptic Curve Cryptography**
   Elliptic Curve Cryptography (ECC) is based on an algebraic structure of elliptic curves over finite fields. While RSA keys are based on the mathematical intractability of factoring a large integer of two or more prime factors, ECC assumes that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible. For current cryptographic purposes, an elliptic curve is a plane curve which is made up of points satisfying the equation: y2=x3+ax+n, along with a distinguished point at infinity (∞). The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated. This set together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.

   At the RSA Conference 2005, the National Security Agency (NSA) announced Suite B which exclusively uses ECC for digital signature generation and key exchange. The suite is intended to protect both classified and unclassified national security systems and information.

3. **NIST Recommended Key Sizes**
   NIST stands for “National Institute of Standards and Technology” which is a U.S. federal government “technology agency that works with industry to develop and apply technology, measurements, and standards.” NIST recommendations are part of the standards ecosystem that web browsers and CAs abide by.

| Minimum size (bits) of Public Keys | | | | Key Size Ratio |
|---|---|---|---|---|
| Security (bits) | DSA | RSA | ECC | RSA/DSA to ECC |
| 112 | 2048 | 2048 | N/A | 1:09 |
| 128 | 3072 | 3072 | 256-383 | 1:12 |
| 192 | 7680 | 7680 | 384-511 | 1:20 |

The practical advantages of a smaller key size compared to the equivalent-security larger key size are an increase in server performance and the number of simultaneous connections possible, combined with a decrease in CPU usage.

# The on-going challenge

The DES key is 56 bits and so there are 2 to the power of 56, or approximately 7 quadrillion (7 x 1016) combinations, which makes it virtually impossible to decrypt. However, due to the significant increase in computing power, decryption was finally achieved in 1994.

Similarly, the cryptographic algorithm used in TLS/SSL is not impossible to decrypt, but simply renders decryption impossible within a realistic timescale and cost framework based on today's computing power. So, to avoid the same fate as the DES key, the specification for TLS/SSL public key length was changed from 1,024 bits to 2,048 bits. A new move towards a TLS/SSL SHA2 digital signature for public keys has also recently gained more prominence as corporations considering their response to the Payment Card Industry Data Security Standard (PCI DSS).

Users of TLS/SSL encrypted communications have upgraded PC browsers, mobile telephones, smart phones and other client devices, as well as web browsers, to respond more quickly to new hash functions and key length. However, the on-going maintenance of encryption strength remains a priority.

NIST recognised the limitations of the current RSA1024 bit certificate key size used in TLS/SSL and issued a deadline for switching to 2048-bit certificates by January 2014. The move to 2048 bit certificates help address the many of the security concerns, attacks against a particular key size have become more practical as computing power increases and new techniques have been developed – however the increase in the RSA key size can have a negative impact on server loads, and the number of possible concurrent connections. An alternative option is to use Elliptic Curve Cryptography (ECC) which creates encryption keys based on the idea of using points on a curve to define the public/ private key pair. With ECC it is difficult to break using the brute force methods and potentially offers a faster solution with less computing power than RSA-based encryption.

As with all other ciphers, the cryptography used in TLS/SSL can only maintain its on-going effectiveness, if browsers, servers and TLS/SSL server certificates stay in lock-step with rising cryptographic power. So it is important for users and providers alike to recognise that such ciphers will be decrypted if adequate steps are not taken to ensure that the appropriate safeguards are always in place – which would have a serious impact on the very use of the Internet.

## But the future is bright

As we have seen, the history of cryptography is a cycle of invention of a new cryptographic algorithm, followed by the invention of a new decryption method. A noteworthy milestone within this progression is quantum cryptography, which uses the angle of oscillation of a photon of light to receive encrypted information.

Whereas previous ciphers were undecipherable in a realistic timeframe, quantum ciphers are said to be impossible to decrypt, because any interception of the data causes the angle of photon oscillation to change, so it is easily detected.

## References

Simon Singh: The Code Book; Shinchosha Publishing Co., Ltd. 2001

http://freemasonry.bcy.ca/texts/templars_cipher.html
http://www.nsa.gov/ia/programs/suiteb_cryptography/
http://www.nsa.gov/public_info/_files/cryptologic_spectrum/early_history_nsa.pdf

For more information, email our security experts at contactus@digicert.com

## Americas

**Lehi, USA**
2801 North Thanksgiving Way, Lehi, Utah 84043, USA

**Mountain View, USA**
485 Clyde Ave., Mountain View, California 94043, USA

## Asia Pacific, Japan

**Bangalore, India**
RMZ Eco World, 10th Floor, 8BCampus,
Marathalli Outer Ring Road, Bangalore - 560103, India

**Melbourne, Australia**
437 St Kilda Road, Melbourne, 3004, Australia

**Tokyo, Japan**
Ginza Six 8F, 6-10-1 Ginza Chuo-Ku, Tokyo,
104-0061, Japan

## Europe, Middle East, Africa

**Amsterdam, Netherlands**
Nevelgaarde 56 Noord, 3436 ZZ Nieuwegein,
Netherlands

**Cape Town, South Africa**
Gateway Building, Century Blvd & Century Way 1,
Century City, 7441,Cape Town, South Africa

**Dublin Ireland**
Block 21 Beckett Way, Park West Business Park,
Dublin 12, D12 C9YE, Ireland

**Gallen, Switzerland**
Poststrasse 17, St Gallen, Switzerland, 9000

**London, England**
7th Floor, Exchange Tower,
2 Harbour Exchange Square, London E14 9GE

**Mechelen, Belgium**
Schaliënhoevedreef 20T, 2800 Mechelen, Belgium

**Munich, Germany**
Ismaninger Strasse 52, 81675 Munich, Germany

digicert®