



Encryption I

An Introduction



Reading List

- ADO and SQL Server Security
- A Simple Guide to Cryptography
- Protecting Private Data with the Cryptography Namespaces
- Using MD5 to Encrypt Passwords in a Database
- Building Secure ASP.NET Applications



Cryptography

- An _____ science that was originally used for military communications and designed to _____
_____ should it fall into the hands of the enemy.



Cryptography

- Recent Implementations

- Authenticating network users
- Ensuring _____

- Preventing users from rejecting ownership of their transmitted messages
- Secure Communications



Encryption

- The name given to the process of _____, which scrambles the data in it—making it very difficult and time consuming, if not practically impossible, to deduce the original given only the encoded data.



Encryption

○ Keys

- Inputs to the encryption algorithm typically involve additional _____ called keys.
- Prevents the message from being _____, even if the algorithm is publicly known.



Encryption

- Safekeeping of Keys
 - Protect them
 - _____, _____, _____ of keys must be protected
 - An encrypted message with a known Key is not encrypted at all



Encryption

- Strength of an encryption

- Dependent on two factors:

- Nature of the _____

- _____ of the Keys involved



Encryption

○ Hacking

● Brute Force

- Trying every possible key until the decrypted message has been found.

● 40-bit encryption standard (until recently)

- Easily broken by Brute Force

● 128-bit encryption

- Now required to ensure confidence



Types of cryptography

- Symmetric Cryptography – Secret Keys
 - Same Key is used for both encryption and decryption
 - _____
 - Problem:
 - The receiver needs the key.
 - How do you get the key to them, securely?
 - Weakness of symmetric cryptography.



Symmetric Cryptography

○ Plain Text \rightarrow Algorithm \rightarrow CipherText

○ Plain Text \leftarrow Algorithm \leftarrow CipherText

- The decryption key on the bottom is identical to the encryption key on the top.



Types of cryptography

- Asymmetric Cryptography \tilde{A}, \hat{A} – Public/Private Keys
 - Uses 2 keys that are mathematically related
 - _____ Key – Never revealed
 - _____ Key – Freely given out



Asymmetric Cryptography

- Public / Private Keys
 - If the keys are long enough, it is practically impossible to determine one from another
 - Processing required is CPU intensive
 - Potential performance problems



Asymmetric Cryptography

- RSA – Public/Private Key algorithm
 - Named for Rivest, Shamir, Adleman
 - Patented by RSA Data Security in '77
 - Sender uses Receiver's public key to encrypt
 - Only the receiver with the related private key can decrypt it



Asymmetric Cryptography

- Digital Signature

- A form of RSA

- Sender encrypts the message using their private key
 - Anybody can decrypt the message using the sender's public key
 - Meaning:
 - The sender, who is the only person in possession of the private key, must have sent the message



Message Digest

- Digital fingerprint of a message
- Derived by applying a mathematical algorithm on a variable-length message
- Use a hash function



Hash functions

- A *hash function* H is a transformation that takes an input m and returns a fixed-size string, which is called the hash value h (that is, $h = H(m)$).



Hash functions

- Basic Requirements:
 - The input can be of any length.
 - The output has a fixed length.
 - $H(x)$ is relatively easy to compute for any given x .
 - $H(x)$ is one-way.
 - $H(x)$ is collision-free



Message Digest

- Use message digests to guarantee that no one has tampered with a message during its transit over a network.
- If the message has been tampered with, the message and the digest will not correlate.



Hash functions

- Well known message digest hash functions:
 - MD2
 - MD4
 - _____
 - Secure Hash Algorithm (SHA)



MD2

- Developed by Rivest in 1989.
- The message is first padded so its length in bytes is divisible by 16. A 16-byte checksum is then appended to the message, and the hash value is computed on the resulting message.



MD4

- Developed by Rivest in 1990.
- The message is padded to ensure that its length in bits plus 64 is divisible by 512. A 64-bit binary representation of the original length of the message is then concatenated to the message. The message is processed in 512-bit blocks in the Damgård/Merkle iterative structure and each block is processed in three distinct rounds.



MD5

- Developed by Rivest in 1991.
- It is basically MD4 with "safety-belts" and while it is slightly slower than MD4, it is more secure
- The algorithm consists of four distinct rounds, which has a slightly different design from that of MD4. Message-digest size, as well as padding requirements, remain the same.



SHA

- Developed by the National Institute of Standards and Technologies (NIST)
- The algorithm takes a message of less than 2^{64} bits in length and produces a 160-bit message digest. The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks



DES

- Symmetric Encryption Algorithm
- Data Encryption Standard
 - Published in 1977 by the National Bureau of Standards.
 - Became an ANSI standard.
 - Single DES is permitted only for legacy systems.



Triple DES

- Symmetric Encryption Algorithm
 - The latest Federal Information Processing Standard (FIPS) which describes the DES includes a definition for Triple-DES.
 - TDEA is "the FIPS approved symmetric algorithm of choice."
 - Within a few years, DES and triple-DES will be replaced with the AES



Triple DES

- The idea behind Triple DES is to improve the security of DES by applying DES encryption three times using three different keys.
- This way the effective key length becomes $56 \times 3 = 168$ bits which makes brute-force attacks virtually impossible.



DES & TDES

- Has DES been broken?
 - No easy attack on DES has been discovered, despite the efforts of researchers over many years.
 - The obvious method of attack is a brute-force exhaustive search of the key space; this process takes 255 steps on average.



AES

- Symmetric Encryption Algorithm
- Advanced Encryption Standard
 - Successor to _____
 - Published in November of 2002
 - Published by _____
 - Intent:
 - To have a cipher that will remain secure well into the next century.



AES

- AES supports key sizes of 128 bits, 192 bits, and 256 bits, in contrast to the 56-bit keys offered by DES.
- Over time, many implementations are expected to upgrade to AES, both because it offers a 128-bit key size, and because it is a federal standard.



AES Algorithm - Rijndael

- NIST selected Rijndael as the AES algorithm.
- The algorithm's developers have suggested the following pronunciation alternatives:
 - "Reign Dahl", "Rain Doll", and "Rhine Dahl".

RSA SecurID



- RSA SecurID two-factor authentication is based on:
 - something you _____ (a password or PIN) and
 - something you _____ (an authenticator)
 - providing a much more reliable level of user authentication than reusable passwords.

RSA SecurID



- Provides user authentications options for:
 - VPNs
 - Wireless Communications
 - Email
 - Intranets, Extranets
 - Web Servers
 - Other...



SQL Server Encryption

- SQL Server has built-in encryption to protect various types of sensitive data.
- In some cases, this encryption is completely transparent to you; things are encrypted when they're stored and decrypted automatically when they're used.



SQL Server Encryption

- In other cases, you can choose whether data should be encrypted or not. SQL Server can encrypt the following components:
 - Passwords
 - Definitions of stored procedures, views, triggers, user-defined functions, defaults, and rules
 - Data sent between the server and the client



SQL Server Encryption

- SQL Server automatically encrypts the passwords that you assign to logins and application roles.
- Even if you look directly into the system tables in the master database, you won't find actual passwords.
- You don't need to do anything to enable this feature; in fact, you can't disable it



SQL Server Encryption

- You may have noticed something obviously missing from this list of things that can be encrypted: the data in your tables.
- SQL Server doesn't offer any built-in support for encrypting your own data before you store it.



Further Research

- <http://www.rsasecurity.com>
- <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/secnetlpMSDN.asp>



Moral of the Story

- Some encryption is better than no encryption at all.
- When possible, encrypt sensitive data