SECURITY BRIEF

MerlinCryption™

Protect Your Privates

Algorithmic Innovation Antiquates Standard Encryption

AES-256 bit encryption is a sinking ship in dangerous waters, making private data an easy feast for cyber sharks.

This security brief exposes the leaky hull of standard encryption and presents a unique watertight method to seal stored and shared communications from harm.

Today's criminals are sophisticated, devious, and more technically armed than ever. They no longer go after *only* "big fish." With minimal effort, they can catch everything in the sea. All of us, whales *and* minnows, need highly advanced encryption to outsmart this new breed of shark.

Most encryption programs use the same basic algorithm. The method is common knowledge and widely used, which is why it's called 'standard encryption.'

These off-the-shelf programs are repackaged in different security products. Their 'secrets' are published for all to see.

Standard programs generate standard keys typically limited to a 256-bit key length. These short keys repeat over and over in the cipher-text. The length of a standard key does not change. Published algorithms and short, fixed keys give hackers the clues they need to spot the key, break the code, and access confidential information.

Continued…

DATA-IN-USE • DATA-IN-MOTION • DATA-AT-REST

MerinEZ

Securely store and transfer airtight files anywhere, even on unsecured WiFi and media

MerinEye

Access password lists and on-screen activities, while blocking key-loggers and onlookers

Merlin4Chat

Say it all and reveal nothing! Share and chat on IM, Skype, P2P, email, and in the cloud… It's safe

MerlinFusion

Master business complexity and client nuances with flexible options and access control.

©

Think Different, Do Different, Get Different Results
Change Your Approach For Radical Safety

MerlinCryption's innovative method is fundamentally different from AES-256, or any other encryption on the market, today. With breakthrough cryptography, this unpublished algorithm and key technique drive significant change in data security and introduce a new paradigm to the encryption industry.

Most encryption initiates a key from *inside the program.* The program controls where the key is stored and how it is transferred to others. Computer power can track it down and expose it. In a structural switch, MerlinCryption allows users to design a discrete key and creatively store or exchange it. This unconventional maneuver leverages vast unpredictability.

NEW GAME. NEW RULES. SAFETY WINS!

- Keys scale in size between 2000 bits to 2 gigabytes
- Key-in-a-File methodology skyrockets unknown variables
- Not based on mathematical technique
- Not subject to normal statistical analysis

Standard encryption uses a strand of digital values to serve as the key. MerlinCryption's approach is radically different, using the digital contents of a data file to make the encryption key. This embedded and variable Key-in-a-File technique is called a CryptoFile™. This powerfully effective answer to intrusion makes it possible for users to create keys up to a massive 2GB in length.

The CryptoFile's™ stealthy technique insures undetectable data and overcomes the leaky limitations of standard encryption.

Other Encryption Keys	CryptoFile™ Key Ingenuity
• Are simple key strands. Hacking forensics easily locate these keys.	• Uses existing content as an embedded key sequence hidden within a file. This Key-in-a-File strateegy has shapeshifting attributes and is nebulous to hackers.
• Have short, fixed key lengths which repeat and repeat. These keys are easily cracked.	• Delivers keys of varying length, up to a massive 2GB in size. The larger the key, the harder it is to crack.
• Are initiated by the encryption program. This is predictable and recognizable to hackers.	• Keys are initiated by the user. Merlin-users choose their own CryptoFile™ from a source outside the program. Impossible to predict by attackers.
• Are exchanged and stored through automated complex systems. These keys can be detected and tracked.	• Merlin-users determine key exchange, as well as where they keep their keys. CryptoFile™ exchange and storage are unknown to anyone but the user.

MerlinCryption LLC
PO Box 341133 | Austin, TX 78734

512-348-SAFE
www.MerlinCryption.com

©

CryptoFiles:
Defiantly Different… Exponentially Secure

'Hack Attack' headlines the news on a daily basis, while persistent threats are cracking the security blockades of industry powerhouses and government fortresses at an alarming rate. Employing a divergent approach to the malicious hacking stratagem, the CryptoFile™ protects privacy with a straightforward Key-in-a-File tactic that stops the intruders in their tracks. Compare the advantage…

Standard	MerlinCryption	
256 Bit (fixed) Keys	2000 Bit to 2 GB (changing) Keys	*User Advantage*
PUBLISHED CODE: Encryption algorithm is known to anyone. Standard code is repeatedly re-packaged as different software and sold as various solutions.	**PROPRIETARY ALGORITHM: MerlinCryption's revolutionary approach is radically different from any other encryption product available. Code is unpublished and private.**	Unknown code and stronger encryption fortifies security. Hackers dont know how to break it.
SINGULAR KEY STRANDS: Uses a simple *fixed* key to encrypt. Hackers have the "known" factors to work with.	**CHANGEABLE KEY TECHNIQUE: Uses a *variable* key, selected from the existing content of the CryptoFile™ by the user. Only Merlin protects you with groundbreaking key ingenuity.**	Variables increase possibilities of keys and unknown factors beyond traceability. Renders hacking useless.
SMALL FIXED LENGTH KEYS: A standard encryption key is typically 128, 256, or 512 bits in length. The length is fixed as dictated by the programming code.	**MASSIVE VARIABLE LENGTH KEYS: Keys can be any length! The minimum key length is 2000 bits; the largest over 17,000,000,000 bits (2GBs). Only Merlin-users control key length. You can change it on a whim.**	Only you know how big the key is up to 2 GBs in size. Hackers need a billion times a billion times (times a billion 67 times) chances to guess it with the smallest key. (Criminals go for easier prey)
BREAKABLE: Keys based on standard mathematical factoring and can be reversed by computers. Hackers apply techniques to factor it.	**NOT COMPUTABLE: Keys do not depend on any known mathematical technique.**	Computers can't crack it. Brute Force can't hack it.
DETECTABLE: Short keys repeat, allowing for analysis based on sequence and frequency of numbers, letters, and symbols. Easy to identify and break.	**UNSYSTEMATIC: Encrypted files are not subject to normal statistical analysis.**	Reverse engineering is futile. Unpredictability reinforces protection and ensures your privacy!
TRACEABLE: Many standard programs use public keys and central key deposits.	**ARBITRARY: Merlin-users creatively choose and control keys and how they are communicated.**	NO key management required. Ends the IT nightmare.
IMPRACTICAL: Recipients of encrypted files must own a corresponding decryption program or use a service to decrypt.	**SEAMLESS PROCESS: Your recipients get a FREE MerlinReader decrypt-only program.**	You have freedom to send secure files to anyone, anywhere, and in any manner. Your recipient need not buy anything to decrypt your file.

Bottom Line: You can *play* it safe with standard encryption or you can *be safe* with MerlinCryption.

Encryption Solutions for Ironclad Data Privacy

MERLINEZ: Protection for data file storage and transfer… simply
MERLINFUSION: Protection for business versatility and client needs
MERLINEYE: Protection for password and data-in-use activity
MERLIN4CHAT: Protection for instant messaging, email, and broadcast
Customization and unique solutions for individual specification

Learn why MerlinCryption's breakthrough encryption architecture is changing the way the world protects and manages data communications. Get safe! Contact us, today.

MerlinCryption LLC
512-348-SAFE
PO Box 341133 | Austin, TX 78734
www.MerlinCryption.com

©