PO Box 20,
Dallas Victoria 3027
Australia

http://www.nightwing.com.au/FileMaker
vox +613 9309 1434
fax +613 9309 8273

INTRODUCING

DataVaultMaker® 2.0 Lite

For FileMaker™ Pro Developers

Product Overview & Specifications

July 2004

Prepared by R J Cologon, PhD
Director of Development,
NightWing Enterprises

PRODUCT DESCRIPTION:

The NightWing Enterprises DataVaultMaker 2.0 Lite is a mini FileMaker application containing two custom functions plus details pertaining to their installation and use in a FileMaker solution. The purpose of the functions is to add the ability to encrypt and decrypt data within the end-user FileMaker database, such as usernames, passwords, codes or sensitive information.

Product Scope
The DataVaultMaker system is structured around the requirements of database applications created with FileMaker Pro version 7. It consists of a unique matched pair of compound formulae in the form of recursive custom functions, for the efficient management of secure storage of passwords and other sensitive data within FileMaker databases.

Since DataVaultMaker is capable of generating multiple unique cryptosystem formula pairs (encoding/decoding pairs), cryptosystems can be particular to a specific database or database function and multiple separate cypher formulae can be deployed for different purposes within one or several database applications.

The cryptographic system uses a custom-designed process which incorporates:
- primary support for an 82-part character set.
- optional custom character sets for scientific, specialist or foreign language data
- support for extended character sets (more than 82 chars) via secondary processing
- authentication of encoded data packets for tamper-proofing.
- Provision for secure password protection of the encrypted string.

Practical Applications
Despite the increased security afforded by the revised file architecture in version 7 of FileMaker Pro, there is an ongoing need to protect sensitive information from possible unauthorised access. Whether storing authentication data within the database itself or storing information which is subject to privacy or confidentiality concerns, encryption provides a way of storing data with increased confidence.

In the past, various measures have been used to obscure or secrete passwords and other sensitive data – however these have commonly been weak and often inefficient in implementation. Thus both personal privacy and commercial security have been exposed to vulnerabilities.

Because DataVaultMaker 2.0 Lite provides ready-to-use formulae ready to reference directly in FileMaker calculations, it will enable developers to achieve a more secure and professional method of storing sensitive data. This has the potential to provide more flexible user authentication options and added safeguards against unauthorised access to database contents.

Operational Parameters
DataVaultMaker encoding/decoding formula pairs each use the same general framework, but are differentiated by their dependence upon unique and randomly generated cypher keys. The keys are not binary, but rather, are rendered in unicode format suitable for inclusion in and interpretation by the FileMaker Pro calculation engine.

DataVaultMaker 2.0 Lite offers each registered user a unique custom built cryptosystem which will encrypt and decrypt information stored in the FileMaker Pro standard time, date, timestamp, number and text data formats. Its default character set is composed of 82 characters which include numerals 0 to 9, upper and lower case alphabetic characters, plus:
- spaces, carriage returns, commas, periods, colons, semicolons, hyphens, apostrophes, asterisks, brackets, exclamation marks, question marks, ampersands, underscores, 'at' glyphs, pipes, forward slashes and back slashes.

Specialised and extended character sets can be user-specified on an individual cryptosystem basis, to provide for the requirements of specialised applications.

The DataVaultMaker 2.0 Lite functions are designed to operate efficiently within both stored calculations and scripts created in FileMaker Pro and may also in be used in auto-entry calculations. Once installed in a file, the custom functions and the encryption keys that are embedded in them can be stored securely, protected by FileMaker 7's robust security architecture.

DataVaultMaker generates encrypted data strings which are composed of selected characters from the unicode character set. These are combined in packets which incorporate hash-based checksum authentication and correspond to source data by a variable ratio of 1.1 or greater.

The system lends itself to the encoding of strings of unlimited length – up to 200,000 characters of text in a single pass. However short elements can also be efficiently encrypted (eg codes, passwords, numbers etc). Being designed specifically for database use, the system does not incorporate features expected in a messaging protocol (eg public/private key structure, header data etc) but it does make provision for a password at encryption, which is validated via a one-way has and incorporated in the keys used to encrypt the supplied data.

General functionality
DataVaultMaker 2.0 Lite is provided in the form of a mini database which stores the background information required to install and use a single cryptosystem, an example of the cryptosystem in demonstration mode, plus the code for the cryptosystem itself..

Technical Background
DataVaultMaker is written with the FileMaker Pro Developer Edition, and is dependent upon the FileMaker Pro 7 database environment which is available for Windows 2000/XP or later and MacOS X 10.2.8 or later.

The cryptographic tools implemented in DataVaultMaker do not reside in source code, but in high level function code supported by FileMaker. For this reason, the cyphers do not conform to established encryption standards, but utilise a proprietary encryption framework developed for the purpose by NightWing Enterprises.

This has the advantage of making the secured data strings generated by DataVaultMaker less susceptible to hacking techniques developed for other more prevalent encryption standards. As a custom and proprietary system, it operates within an independent framework and exploits the particular strengths and operational parameters of the FileMaker Pro development environment.

The generation of keys and initialisation vectors for the cryptographic procedures harnesses the existing FileMaker Pro 'Random' function, yet is applied via proprietary methodology through which seeding artefacts are filtered to provide a robust encryption architecture.

Given the nature of the environment, the encryption procedure is not rendered in binary form, but is instead manipulate4d and stored at a high level within the FileMaker calculation engine, dealing directly with unicode data rather than raw binary data. For this reason encryption key lengths are not directly comparable to binary keys, but can be equated through formulaic comparison.

The cryptographic process is multi-stage utilising three independent keys to render opaque data strings. The multi-stage process includes:
- source interpolation against one of the keys
- optional password hashing of encryption keys
- bipolar, patterned and randomised register shifting of the interpolated code
- scatter offset of polar-shift factors by character position
- restructuring of the interpolated, shifted and offset code against a second key
- re-initialisation of vectors at content intervals
- modular and vector-based randomization of packet fill
- packeting of encoded sub-strings, rendered against a third cypher key
- internal self-authentication of composite sub-string packets

DataVaultMaker®

PRODUCT SPECIFICATIONS:

Purpose of product	To provide intra-database functionality for secure storage of passwords, user authentication data and/or or other data of a highly sensitive nature.
Scope of end use/application	FileMaker Pro databases and runtimes
Development Environment	FileMaker Developer 7.0v2 or later
Operating systems supported	Windows 2000 Windows XP MacOS X
Hardware recommendations	Intel Pentium 1Ghz or higher, 256Mb RAM or greater, 80Mb or more free hard disk space, or Apple G4 800 or higher, 256Mb RAM or greater, 80Mb or more of free hard disk space
Cryptosystem	Unique per registered user
Maximum string length	200,000 characters per single pass Unlimited* in scripted multiple passes
Distribution options	Unlimited within locked solutions only
Cryptographic process	Multi-process custom encryption process rendered via high level ascii manipulations
Cryptographic efficiency	Generation of codes is hardware dependent, but typically better than 1k/sec. **
Software architecture	FileMaker Pro runtime
Encryption strength***	Interleaving key 20bit (ascii, not binary) Interpolation key 82bit (ascii, not binary) Rendering key 140bit (ascii, not binary)

---

* except as regards limits imposed by available file storage space.

** the estimated encoding speed is an approximation and is based on mid-range PC performance levels (ie 1.5Ghz or less).

*** cipher keys are generated directly into unicode and are therefore not directly comparable to binary keys of equal length. However in base conversion, the equivalent strength is equal or greater than binary keys of the same length.

Document prepared by:
R J Cologon PhD
NightWing Enterprises
July 2004