



**Ultra High Speed USB v2.0 Flash Drive with  
448-bit Blowfish ESP (Encryption Software Protection)**

*Where Advanced Data Security Meets High Performance Flash Technology*



**Introduction:**

Axiom's Ultra High Speed E.S.P. Drive (Encryption Software Protection) with 448-Bit Blowfish Encryption Technology is the best solution for data security on the go. Blowfish is one of the strongest and fastest encryption applications in public use, making it ideal for a product like the E.S.P. Drive.

By using a 64-bit block size and 448-bit key length, you can feel safe storing your information and carrying it around with you. It's unique software give users the choice of which data they want to protect while leaving a portion of the drive to act as a standard USB key without having to re-partition. Simply drag and drop the files you'd like to protect into the secured folder, set up your password and feel at ease knowing that your work is protected.

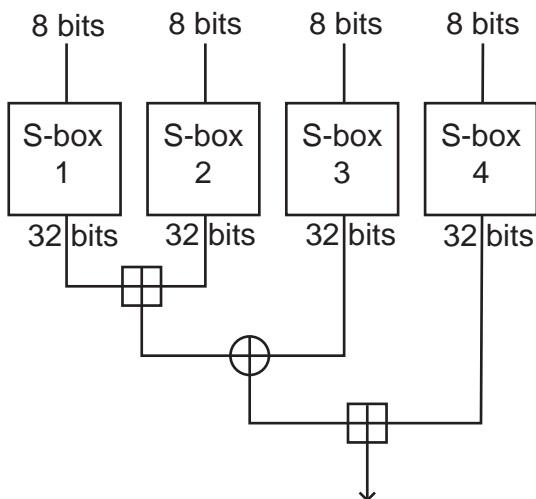
The E.S.P. drive utilizes software based encryption combined with Ultra High speed flash to provide one of the fastest and most secure USB v2.0 Flash devices on the market today.

**About 448-bit Blowfish Encryption:**

The Blowfish algorithm is a keyed, symmetric block cipher designed in 1993 by Bruce Schneier. It was developed as a general purpose algorithm, intended as replacement for the aging DES and free of the problems associated with other algorithms. Blowfish has been analyzed extensively and gone through years of peer review. At no point since it's initial release in 1993 has the Blowfish code ever been cracked. A notable feature of it's design include key-dependent S-boxes and a highly complex key schedule.

Data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

diagram 1

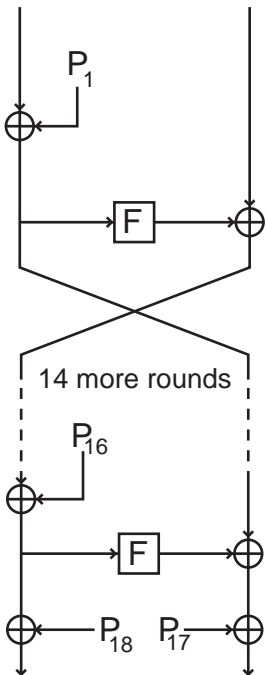


(Diagram 1) shows the action of Blowfish. Each line represents 32 bits. The algorithm keeps two subkey arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed\* with one of the two remaining unused P-entries.

The round function (Feistel function) of Blowfish

\*XOR-exclusive disjunction is a logical operation on two logical values, typically the values of two propositions, that produces a value of true just in cases where the truth value of the operands differ.

diagram 2



The Feistel structure of Blowfish

(diagram 2) shows Blowfish's F-function. The function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo  $2^{32}$  and XORed\*\* to produce the final 32-bit output.

Since Blowfish is a Feistel\*\*\* network, it can be inverted simply by XORing  $P_{17}$  and  $P_{18}$  to the ciphertext block, then using the P-entries in reverse order.

Blowfish's key schedule starts by initializing the P-array and S-boxes with values derived from the hexadecimal digits of pi, which contain no obvious pattern. The secret key is then XORed with the P-entries in order (cycling the key if necessary). A 64-bit all-zero block is then encrypted with the algorithm as it stands. The resultant ciphertext replaces  $P_1$  and  $P_2$ . The ciphertext is then encrypted again with the new subkeys, and  $P_3$  and  $P_4$  are replaced by the new ciphertext. This continues, replacing the entire P-array and all the S-box entries. In all, the Blowfish encryption algorithm will run 521 times to generate all the subkeys - about 4KB of data is processed.

### Strength:

The relative strength of the encryption algorithm is based on key length. Bruce Schneier, creator of the Blowfish encryption algorithm, has calculated that according to what we know of quantum mechanics today, that the entire energy output of the sun is insufficient to break a 197-bit key.

As a more generalized example, the most common key lengths used by today's web browsers are "40-bit" and "128-bit." As a comparison, a 40-bit key can be "cracked" within a few hours by an average personal computer. However, a 128-bit key would take one BILLION powerful computers, each capable of trying one BILLION keys per second. In other words, it would take MILLIONS of years to try every possible combination of bits in a 128-bit key.

In the preceding example, the 128-bit encryption is not just three times stronger than 40-bit encryption — it is 309,485,009,821,345,068,724,781,056 times stronger. Performing this same analysis on a 448-bit encryption key yields an encryption strength that is  $2.1 \times 10^{96}$  times stronger than a 128-bit key.

\*XOR - exclusive disjunction is a logical operation on two logical values, typically the values of two propositions, that produces a value of true just in cases where the truth value of the operands differ.

\*\*Modulo - (sometimes called modulo arithmetic, or clock arithmetic) is a system of arithmetic for integers, where numbers "wrap around" after they reach a certain value — the modulus.

\*\*\*Feistel cipher - is a block cipher with a symmetric structure named after IBM cryptographer Horst Feistel; it is also commonly known as a Feistel network.

\*\*\*Further documentation about the Blowfish algorithm can be found at: <http://www.schneier.com/paper-blowfish-fse.html>

**Flash Drive:**

The Axiom ESP drive offers a Ultra High Speed flash device along with the 448-bit Blowfish encryption software. Generally, there is a tradeoff between the high-speed and more expensive Single-Level Cell (SLC) Flash chips, and the standard speed and more affordable Multi-Level Cell (MLC) or Multi-Bit Cell (MBC) Flash chips. The ESP drive combines only Single-Level Cell (SLC) Flash chips with an optimized, built in NAND Flash memory controller to offer the fastest transfer rates possible.

	ESP Drive	Standard USB Drive
448-bit Blowfish Encryption Software	Yes	No
Single-Level Cell (SLC) Flash chips	Yes	No
Read Speed	125x (18.75MB/s)	65x (9.75MB/s)
Write Speed	65x (9.75MB/s)	15x (2.25MB/s)

Operating System	File Transfer	Data Encryption
Windows Vista	Yes	Yes
Windows XP	Yes	Yes
Windows 2000 (SP3 and above)	Yes	Yes
Mac OS 10.x and above	Yes	No
Linux Kernel 2.4 and above	Yes	No
Win NT, Win 95, Win 98, Win ME	Not Supported	Not Supported

**Other Features:**

- Portable and secure removable mass storage for business and personal use
- Support USB specification version 2.0 and v1.1; true Plug&Play connection
- Support power saving mode to reduce power consumption.
- Shock resistant, noise-free and long data retention
- LED indicator when device is in use.
- Hot Plug and Play.
- No external power is required.
- Dimension:69.6\*17\*10mm(L\*W\*H)
- Weight:10g (+-0.5)
- 5 Year warranty

