

## Encryption Information

### Blowfish Encryption

The Blowfish algorithm developed by Bruce Schneier, is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.

Blowfish is classified as public domain; as such it has been analyzed extensively and gone through years of peer review. At no point since its initial release in 1993 has the Blowfish code ever been cracked. This is significant when you consider that the source code to the algorithm is freely available.

Blowfish supports key lengths of 32 to 448 bits, making it one of the strongest encryption algorithms on the market. Matrosity Hosting uses the Nova Store line of backup software products, which is shipped with 448-bit Blowfish encryption. This is the default encryption setting when the client software is installed.

### Strength

The relative strength of the encryption algorithm is based on key length. Here is a 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 2.1X10<sup>96</sup> times stronger than a 128-bit key.

### Speed

The speed of the algorithm is very impressive. Some may think a 448 bit key length is excessive. However, when we analyze the effective throughput of the

Blowfish algorithm, we see that even large key lengths result in much faster performance than other encryption algorithms.

<b>Speed Comparisons of Block Ciphers</b>				
<b>Algorithm</b>	<b>Clock cycles per round</b>	<b># of rounds</b>	<b># of clock cycles per byte encrypted</b>	<b>Notes</b>
Blowfish	9	19	18	Free, Not patented
Khufu/Khafre	5	32	20	Patented by Xerox
RC5	12	16	23	Patented by RSA Data Security
DES	18	16	45	56-bit key
IDEA	50	8	50	Patented by Ascom-Systec
Triple-DES	18	48		

More information about the Blowfish Encryption Algorithm is available at:

<http://www.schneier.com/blowfish.html>