Encryption-128-bit or 256-bit AES with Swarm-Edge™

Bluetronix Inc. uses either 128-bit or 256-bit AES encryption with its Swarm-Edge™ algorithms to secure their wireless transmissions. Swarm-Edge™ algorithms are based upon patented biological networking capabilities eliminating access points, IP transport and central routers. *How secure is AES with Swarm-Edge™ algorithms?* To answer this question, we refer to the encryption experts as described below:

In the world of embedded and computer security, one of the often debated topics is whether 128-bit symmetric key, used for **AES (Advanced Encryption Standard)** is computationally secure against brute-force attack. Governments and commercial businesses place a great deal of faith in the belief that AES is so secure that its security key can never be broken, despite some of the inherent flaws in AES. This standard is can be put in tandem with Swarm-Edge™ algorithms and the following can be achieved.

Therefore the strength of the *Cryptographic* Swarm-Edge™ *system* against brute force attacks with different key sizes and the time it takes to successfully mount a brute force attack factoring future advancements in processing speeds.

Any cryptographic algorithm requires multi-bit key to encrypt the data as shown in Figure 1.

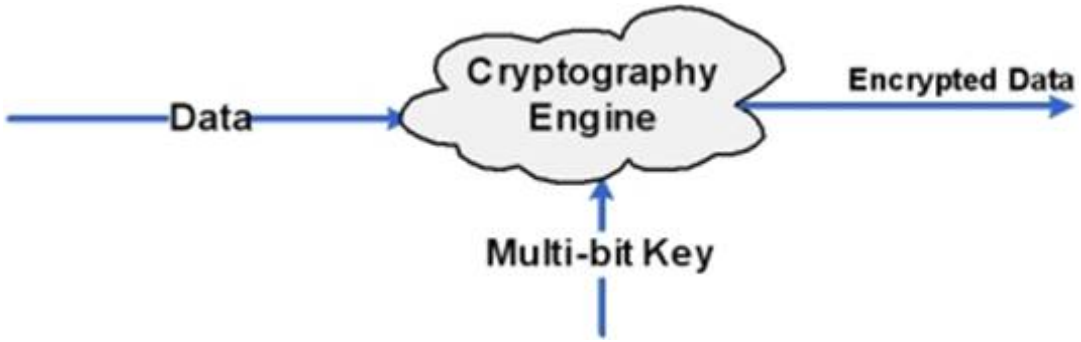
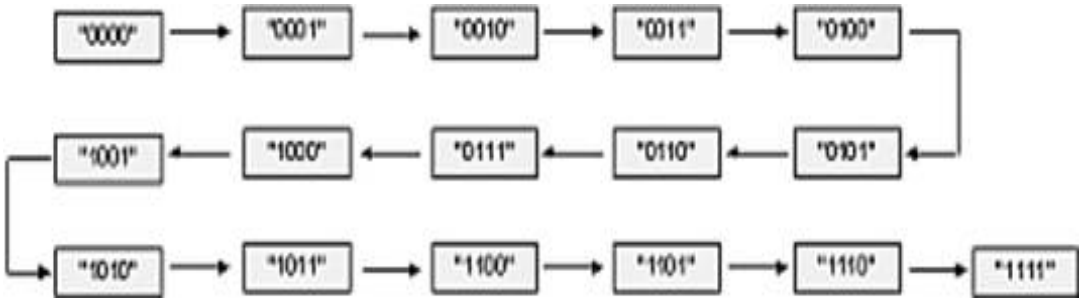


Figure 1: Multi-bit key to encrypt data using cryptographic algorithm

The key length used in the encryption determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones.

Brute-force attack involves systematically checking all possible key combinations until the correct key is found and is one way to attack when it is not possible to take advantage of other weaknesses in an encryption system.

Here is an example of an attack on a 4-bit key:



Voice (440) 247.3434 # 7 Saratoga Crt. Cleveland, Ohio 44122 Fax (440).543.2955
innovation@bluetronix.net www.bluetronix.net

Figure 2: Brute Force attack on 4-bit key

As shown, it will take a maximum 16 rounds to check every possible key combination starting with "0000." Given sufficient time, a brute force attack is capable of cracking any known algorithm.

The following table just shows the possible number of key combinations with respect to key size:

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Figure 3: Key combinations versus Key size see 128-bit & 256 bit

Notice the exponential increase in possible combinations as the key size increases. "DES" is part of a symmetric cryptographic algorithm with a key size of 56 bits that has been cracked in the past using brute force attack. There is also a physical argument that a 128-bit symmetric key is computationally secure against brute-force attack.

Consider the following:

Faster supercomputer (as per ref. Wikipedia): **10.51 Pentaflops = 10.51 x 1015 Flops [Flops = Floating point operations per second]**

#. of Flops required per combination check: 1000 (very optimistic but just assume for now)
# of combination checks per second = (10.51 x 1015) / 1000 = 10.51 x 1012
#. of seconds in one Year = 365 x 24 x 60 x 60 = 31536000
# of Years to crack AES with 128-bit Key = (3.4 x 1038) / [(10.51 x 1012) x 31536000]
= (0.323 x 1026)/31536000
= 1.02 x 1018

= 1 billion billion years *(that's a lot)*

Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

Figure 4: Time to crack Cryptographic Key versus Key size

As shown above, even with a supercomputer, 128-bit with Swarm-Edge™ it would take 1 billion billion years to crack the 128-bit AES key using brute force attack. This is more than the age of the universe (13.75 billion years). If one were to assume that a computing system existed that could recover a DES key in a second, it would still take that same machine approximately 149 trillion years to crack a 128-bit AES key.

Here are more interesting examples. The following snippet is a snapshot of one the technical comparison "*128-bit versus 256-bit AES encryption"* to explain why 128-bit AES is sufficient to meet future needs.

For example if you assume:

Every person on the planet owns 10 computers.
There are 7 billion people on the planet.
Each of these computers can test 1 billion key combinations per second.
On average, you can crack the key after testing 50% of the possibilities.

Then the earth's population can crack one encryption key in
77,000,000,000,000,000,000,000,000 years!

The bottom line is that if AES could be compromised, the world would come to almost a standstill. The difference between cracking the AES-128 algorithm and AES-256 algorithm is considered minimal. Whatever breakthrough might crack 128-bit will probably also crack 256-bit.

In summary, AES has never been know to be cracked yet and is safe against any brute force attacks contrary to belief and arguments. However, the key size used for encryption should always be large enough that it could not be cracked by modern computers despite considering advancements in processor speeds based on Moore's law. Swarm-Edge™ and 128bit or 256 bit AES will provide excellent security for wireless communications and secure connections in most of all wireless applications commercially.