

Re: a few questions about AES

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-10/msg00672.html>

- *From:* Unruh <unruh-spam@xxxxxxxxxxxxxxxx>
 - *Date:* 22 Oct 2006 02:29:12 GMT
-

"Antony Clements" <antony.clements@xxxxxxxxxxxxxxxx> writes:

<snip>

(1) "Complexity". Certainly, the strength of a cipher depends on the algorithm that it uses. But some of these algorithms are amazingly simple – you could write them down completely from memory. So, a "simple" cipher might be very secure, and a "complex" cipher might be trivially insecure. Rather than saying that the strength of a cipher depends on the "complexity", I'd say that the strength depends on the "algorithm (regardless of complexity)".

(2) "How many keys". Phil Carmody put this best. The # of keys establishes an upper bound on the cipher strength. For example, if there are only 2^{10} keys, then, it is trivially easy to try each key in turn (a brute force attack). So, few keys => a weak cipher. But the converse is not necessarily true: many keys does /not/ necessarily => a strong cipher.

<end snip>

the algorithm is very very simple, and i was referring to the complexity of the key(s) used. the algorithm is a simple XOR stream cipher that concatenates each key (each key is = the length of the userkey * 8. the minimum size userkey is 8 bytes the maximum for the userkey is 64 bytes.). this is why i have set a physical limit on the file size so that no keys are repeated. the more permutation techniques AFAIK = more possible keys. the lowerbound of possible keys is 3.43239^{156} by my calculations, with an upper bound of 1.0443^{1233} . keys use the whole ascii range.

<snip>