

## Re: Are natural languages secure ciphers?

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/0475.html>

---

**From:** Paul Schlyter (*pausch\_at\_saaf.se*)

**Date:** 10/05/03

Date: Sun, 5 Oct 2003 10:20:30 +0000 (UTC)

In article <6upunv43i5d8ob4fuov62vcihum68mc063@4ax.com>, Mxsmanic <mxsmanic@hotmail.com> wrote:

> *Dennis Knorr writes:*

>

>> *No! otherwise you could decode AES without a password.*

>

> *The only difference I can see is that encryption keeps part of the algorithm secret (namely, the key), whereas encoding keeps all of the algorithm public.*

The most important difference is that the PURPOSE of the encryption is to keep the input data secret. Thus, in a strong crypto algorithm, changing one bit of the input data will produce a completely different ciphertext. In encoding, changing one bit of the input data will often produce only a small, local, change in the encoded version of the data.

> *ZIP compression is a form of encryption,*

What is "ZIP compression"?

There's no compression algorithm called "ZIP compression". However, the ZIP file compressor and archiver uses four or five different algorithms, choosing the one which produces the smallest compressed version for a particular file. There's even a "compression algorithm" called "Storing" which doesn't compress at all but merely copies the data -- it's there to ensure that the compressed version never grows larger than the uncompressed version of the file.

So, which one of the compression algorithms used by ZIP were you referring to? Perhaps "Storing" ??? <g>

> *but no part of the algorithm is secret and the algorithm is not designed to maximize obfuscation, so it isn't a very useful cipher.*

...thus there are important design differences between compression and encoding.... <g>

sci.crypt: Re: Are natural languages secure ciphers?

--

-----  
Paul Schlyter, Grev Turegatan 40, SE-114 38 Stockholm, SWEDEN  
e-mail: pausch at stockholm dot bostream dot se  
WWW: <http://www.stjarnhimlen.se/>  
<http://home.tiscali.se/pausch/>