

# Re: A Question of Permutations of Vectors of Bits

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-07/2204.html>

---

**From:** Mok-Kong Shen ([mok-kong.shen\\_at\\_t-online.de](mailto:mok-kong.shen_at_t-online.de))

**Date:** 07/31/03

Date: Thu, 31 Jul 2003 09:22:15 +0200

Simon G Best wrote:

>

> *Mok-Kong Shen wrote:*

>>

>> *In the first post you said that P is known and is*

>> *easily invertible. Your second post said that P is*

>> *like a block cipher with a particular key, implying*

>> *(in my understanding) that P is unknown to the person*

>> *solving the question, right? So, after all, is P 'known'*

>> *(i.e. a given particular permutation, fully written out)*

>> *or not? Please kindly clarify.*

>>

>> *M. K. Shen*

>

> *P is known. Therefore, if P happens to be a block cipher's encryption*

> *function with a particular key, the key is not secret.*

Just to assure proper understanding by me: Is P something like in the common notation (parentheses are big)

1 2 3 4

( )

2 3 1 4

and this is known to the problem solver? In that case David Wagner's suggestion to use linear algebra to solve the problem should be the right one. In the other case please again explain with some details.

M. K. Shen