

Re: Coding Theory Question, I think

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-09/msg03032.html>

- *From:* "Rusty" <rusty@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 13 Sep 2005 17:33:26 +0100
-

"Thinus Pollard" <thinus@xxxxxxxxxxxxxxxx> wrote in message [news:dg6cbk\\$cdj\\$1@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:dg6cbkcdj1@xxxxxxxxxxxxxxxxxxxxxxxx)

> Nope, I did some abstract algebra a few years ago where we did some coding
> theory.
>
> The system issues tickets. Each ticket contains a PIN. This PIN needs to
> be
> unique and only I should be able to issue valid PINs.
>
> The PIN contains an issue date, an expiry date, a unique serial number and
> an amount. All this data should be encoded into a 16 *digit* string.
>
> Validation should take the following form:
> 1. When entered the system should check if the entered string is valid.
> This
> is easy, use 15 digits and append a check as the 16th.
> 2. When verified the system should check if the data inside the PIN "makes
> sense".
>
> I was thinking about packing all the data into some bits and then
> encrypting
> it with a cipher (public key or symmetrical). The problem with this idea
> is
> how to map the data to a 15 digit string, without losing information? From
> the 16 digits you should be able to extract the information if you have
> the
> cypher keys.

Keep error correcting coding and cryptography concepts separate.

Error correcting coding in the communications sense would use a Reed-Solomon or BCH code to represent your data as an expanded string of symbols. Any book on coding theory or http://en.wikipedia.org/wiki/Error-correcting_code will have options in the appendix which will fit your requirements. Basically you need a $M \times N$ coding matrix H , $M \gg N$, such that if your data string is N -length vector X the coded output is M -length vector $Y = HX$; the product done in some modulo number field. For an RS code with base 256 you will need three decimal digits or two hex digits to print each symbol.

Re: Coding Theory Question, I think

Decoding in the presence of errors is a bit messy but basic error detection without correction is easy.

To encrypt this coded string, is a different matter, <http://en.wikipedia.org/wiki/Encryption> and depends on the level of protection required.

rusty

• *References:*

- ◆ *Coding Theory Question, I think*
 - ◇ *From:* Thinus Pollard
 - ◆ *Re: Coding Theory Question, I think*
 - ◇ *From:* William Elliot
 - ◆ *Re: Coding Theory Question, I think*
 - ◇ *From:* Thinus Pollard
-
- Prev by Date: *Re: Math is torture !*
 - Next by Date: *Re: infinity*
 - Previous by thread: *Re: Coding Theory Question, I think*
 - Next by thread: *How many games of chess are there?*
 - Index(es):
 - ◆ *Date*
 - ◆ *Thread*