Cryptography

AES – FPE

Format Taiwan ID number

*Check Alphabet table from hand out for letter conversions*

* We will use 8 bit binary for each number. Thus need to determine a padding schema
* Then append 5 bytes of zeros to get 128 bit requirement needed by the AES block cypher
  + 8 \*11 = 88. 128-88=40. 40/8= 5

Example: U800003281

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Weights** | 1 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 1 |  |  |  |
|  | A | | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 8 | 1 | **Pad** |  |  |
|  | 2 | 8 | 1 | 0 | 0 | 0 | 0 | 3 | 2 | 8 | 1 | 5 \* 0 | **Sum** | **%10==0** |
|  | 3 | 72 | 8 | 0 | 0 | 0 | 0 | 9 | 4 | 8 | 1 | 0 | 100 | True |
| **Binary** | 00000011 | 00001001 | 00000001 | 00000000 | 00000000 | 00000000 | 00000000 | 00001001 | 00000100 | 00001000 | 00000001 |  |  |  |
| New Idea with weights(max) |  |  | 1 | 111111 | 110110 | 101101 | 100100 | 10101 | 10010 | 1000 | 1 |  |  |  |
| New new idea without weight | 11 | 1000 | 1 | 1010 | 1001 | 1001 | 1001 | 1001 | 1001 | 1001 | 1 | 36 bits | Try this for truncation |  |

1010001

After Conversion (we have 128 bit number):

BINARY: 00000010 01001000 01000000 00000000 00000000 00000000 00000000 00001001 00000100 00001000 00000001 00000000 00000000 00000000 00000000 00000000

HEX: 02484000 00000009 04080100 00000000

Attempt #1 3 rounds Luby Rack-off construction (same key) Truncated-F from AES block

Other options : 7 rounds with different keys of fiestel (different key) truncated-F from AES block – la Patarin, Crypto’03

Things to know:

<https://www.youtube.com/watch?v=X6opF_ma234>

<https://www.coursera.org/lecture/crypto/format-preserving-encryption-aFRSZ>

<https://www.coursera.org/lecture/crypto/review-prps-and-prfs-9p25F?isNewUser=true>

<https://pycryptodome.readthedocs.io/en/latest/src/cipher/classic.html>

<https://www.youtube.com/watch?v=Lgo7aGWJe60>



