Secure Overt PIN Codes

Erez Kalman
CISSP, ISSAP, CCSP, CSSLP, CISM, CISA, CDPSE, CASP+, CCZT, CCSK

Using military grade cryptography for securing your PIN codes, such as on your personal credit card.

Choosing your key

Pick a secret number that is:

1. Easy for you to remember
2. Hard for anyone to guess
3. Preferably not used anywhere
4. Preferably not related to you or your family (i.e., date of birth, names, pets,...)

We'll Use 2580 In Our Example

Encrypting

Simple calculation

Protect	1234
Secret	2580

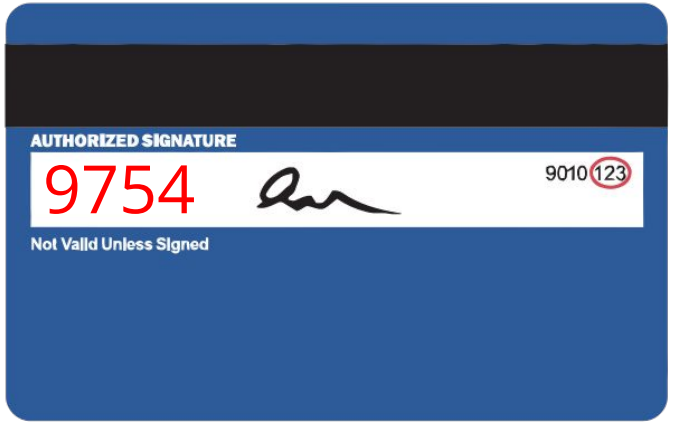
Subtract

1 is smaller than 2 so we add 10 to it before subtracting
1-2 = 11-2 = 9
2-5 = 12-5 = 7
3-8 = 13-8 = 5
4-0 = 4

Result (Encrypted)	9754

Use

We can openly write down the PIN, for example on our credit card and as long as no one knows the “protect” or “secret” values no one can decrypt our code. In the next page we’ll see how we can easily decode it “on-the-fly” whenever we need it.



Decrypting

Simple calculation

Unprotect	9754
Secret	2580

Add

If the result is larger than 9 (i.e., two digits), ignore the left digit

9+2 = 11 = 1
7+5 = 12 = 2
5+8 = 13 = 3
4+0 = 4

Result (Decrypted)	1234