|  |  |  |
| --- | --- | --- |
| Luke Pepin | CSE 4400 - HW 1 | 2/5/2025 |

1. Chip and PIN vs. Chip and Signature:

The main difference between the 2 cards is that chip and PIN cards require a personal identification number for purchase verification while chip and signature require a signature. This difference results in different levels of security leaving Chip and PIN to be more secure since a fraudster requires your exact PIN as opposed to a signature replicate which is an imprecise method of authentication given its variability.

Adopting Chip and PIN provides more security against fraud and is the global standard.

Adopting Chip and signature is easier to transition from magnetic strips and is cheaper to implement.

Sources:

[Chip-and-PIN vs. Chip-and-Signature](https://wallethub.com/edu/cc/chip-and-pin-vs-chip-and-signature/25668)

[Chip-and-PIN Card: Definition, Features, vs. Chip-and-Signature](https://www.investopedia.com/terms/c/chipandpin-card.asp)

1. OpenSSL Encryption:
   1. “data.enc”:

Command: openssl enc -d -aes-256-cbc -pbkdf2 -in data.enc -out data.txt -pass pass:CSE4400-Spring2025

Number near end of plaintext: 1881

* 1. “data.enc” base64:

Command: openssl enc -aes-128-cbc -K ebf01882090b2e6cf9b7e61b0ae5e3fb -iv 5b2f79fbd76b65de872f5abfb8b5375e -base64 -in data.txt -out data.asc

Output: data.asc:

y66q41efvvVZrM1O76WDolGUQ2bnKKQPPRJ9O5M/PZqtdkUwx+ocBsjoHgHXa/kb

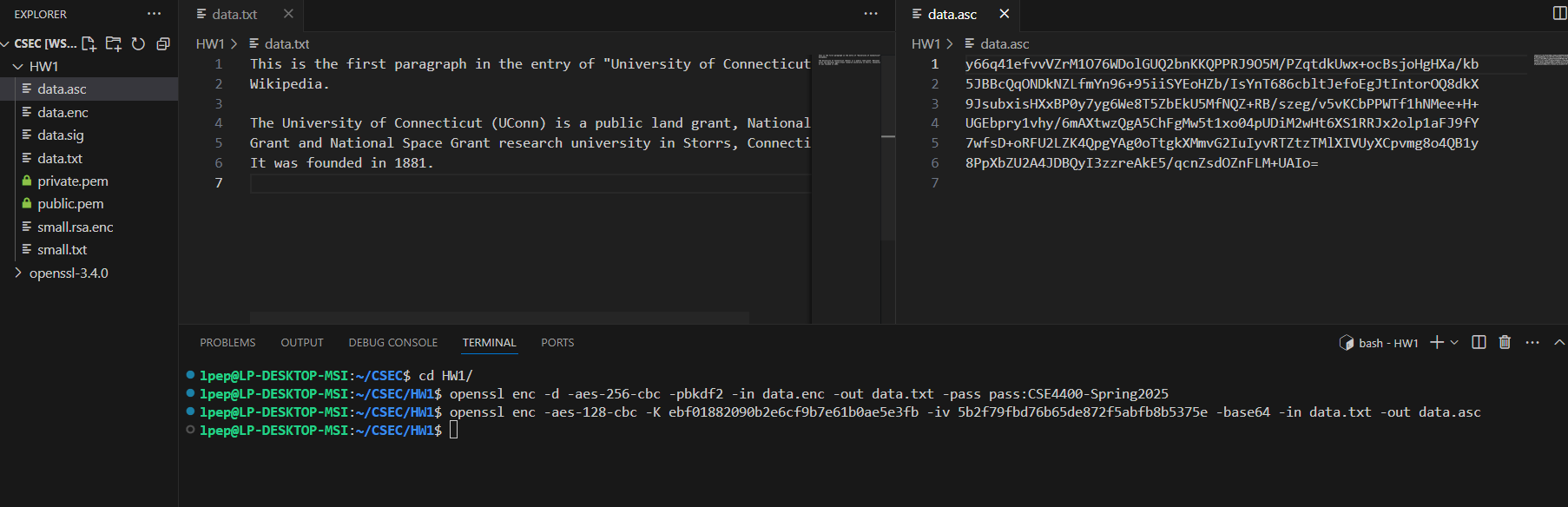
5JBBcQqONDkNZLfmYn96+95iiSYEoHZb/IsYnT686cbltJefoEgJtIntorOQ8dkX

9JsubxisHXxBP0y7yg6We8T5ZbEkU5MfNQZ+RB/szeg/v5vKCbPPWTf1hNMee+H+

UGEbpry1vhy/6mAXtwzQgA5ChFgMw5t1xo04pUDiM2wHt6XS1RRJx2olp1aFJ9fY

7wfsD+oRFU2LZK4QpgYAg0oTtgkXMmvG2IuIyvRTZtzTMlXIVUyXCpvmg8o4QB1y

8PpXbZU2A4JDBQyI3zzreAkE5/qcnZsdOZnFLM+UAIo=



1. OpenSSL Hash
   1. openssl dgst -sha256 data.enc

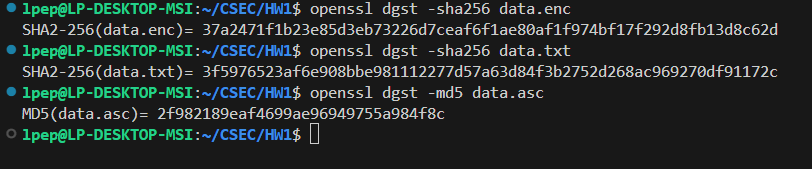
SHA2-256(data.enc)= 37a2471f1b23e85d3eb73226d7ceaf6f1ae80af1f974bf17f292d8fb13d8c62d

* 1. openssl dgst -sha256 data.txt

SHA2-256(data.txt)= 3f5976523af6e908bbe981112277d57a63d84f3b2752d268ac969270df91172c

* 1. openssl dgst -md5 data.asc

MD5(data.asc)= 2f982189eaf4699ae96949755a984f8c



1. OpenSS Public-key
   1. “private.pem”:

openssl rsa -in private.pem -pubout -out public.pem

public.pem:

-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0sG0q3QyUAlF7QYrRURT 69XAsjjsKrpEzVT0x+hH8SyqhEgJo2U4VUk2qrGrSrADDvO1DfQ8TRkCn/+5NDzI g/AqvNaNsYukoc4a5Fm81gla2SrUM+VrapxyTEOLuqIGICRMwpa1lHjnbhSJES1Q w1PWv4qFVNKrarlxm6+nxgwNIsVrTRihPQ+4wVbkGUJFqOwr/VOkq0mijJv8CYLg KWtdWtElK9B9xNqhKg8R4Q0BM9Wu03lq00/rf083MS6nwpMcJ0JrxhvUbRdcrrRH n1gu5YwrzWxSBK75UjXwB6aFaSzo3WS8GC0eYZSAC90iCGqzpT+qr6chyfYu6KYE BQIDAQAB -----END PUBLIC KEY-----

* 1. “small.rsa.enc”

openssl pkeyutl -decrypt -inkey private.pem -in small.rsa.enc -out small.txt

small.txt: 1ce336ed32d8f523633686f1b3ae8576952fe7622b4fda25118c8651c316b359

* 1. “data.enc”

openssl dgst -sha256 -sign private.pem -out data.sig data.enc

openssl dgst -sha256 -verify public.pem -signature data.sig data.enc

Output: Verified OK

