Speed Comparison of Bitwise Hill Cipher

James Corcoran – Final Report
CECS 625 Parallel Programming
Dr. Ouyang
7 April 2013

Intro – The hill cipher is a basic encryption technique that involves the generation of an *n*-by-*n* matrix that serves as the key for the encryption operation. The operation is then performed by multiplying the key by the plaintext in order to obtain the ciphertext; $Ax = b \ (mod\ m)$, where A is the encryption key, x is the plaintext vector, and b is the resulting ciphertext vector. For the decryption operation, A^{-1} will be multiplied by each vector of ciphertext to result in the original plaintext message; $A^{-1}y = c \ (mod\ m)$, where A^{-1} is the inverse of the encryption key, y is the vector of ciphertext, and c is the resulting plaintext.

Project – this project serves as a proof-of-concept for a modified implementation of a hill cipher using two matrix multiplication algorithms: Square-Matrix-Multiply (SMM) and Strassen's algorithm. There is an integer array with values stored as key sizes, where key size = 8, 16, …, 512. Each of these sizes will be used to form an $n \ x \ n$ matrix that will serve as the key. In this project, however, 512 is not implemented due to the difficulties obtaining an inverse matrix for a 512x512 key. Additionally, Strassen's algorithm runtime should not be viewed as accurate because of poor implementation leading to non-optimal results. The program loops through each key, calling *generateKey()* and *decryptKey()* as appropriate. Once the keys are generated, we can start the hill cipher algorithm. This will either implement the Strassen algorithm with the encryption and decryption key, or use the simple Square Matrix Multiplication algorithm using 3 nested loops and the formula $C(i,j) = C(i,j) + (A(i,k) * B(k,j))$. The data is read from a file, and each byte is stored in a two dimensional array that has width equal to the key width, and height equal to the # characters divided by the key width(x). If there is a remainder, 0-padding is used to obtain a height(y) that is perfectly divisible by the key width. Once the characters are stored, they are converted to Ascii values, and then each bit in their binary representation is stored in a different x*y matrix, termed a *bit plane*. Each of the bit planes are then separately encrypted using the Hill cipher.

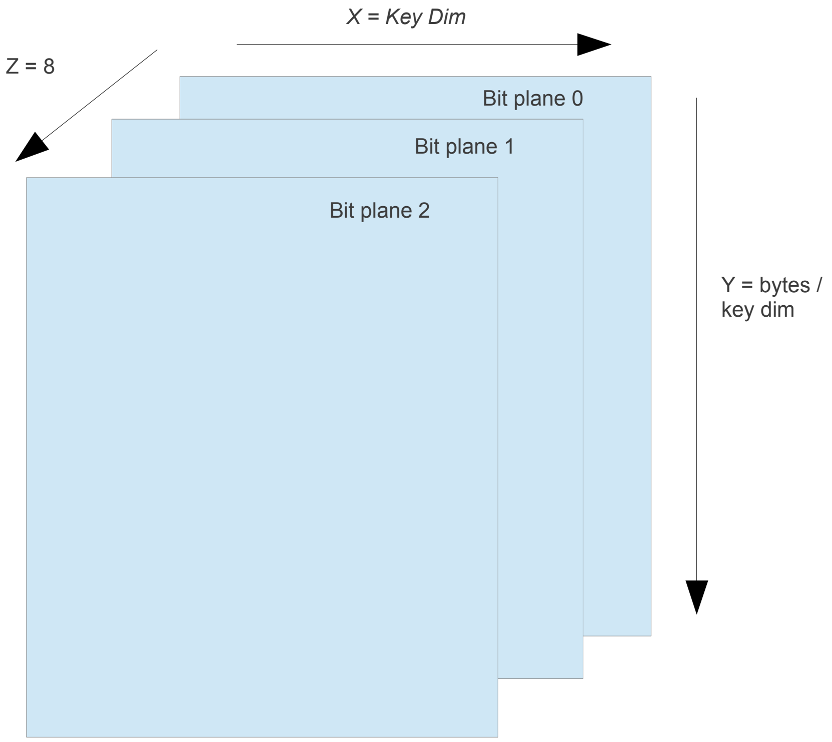


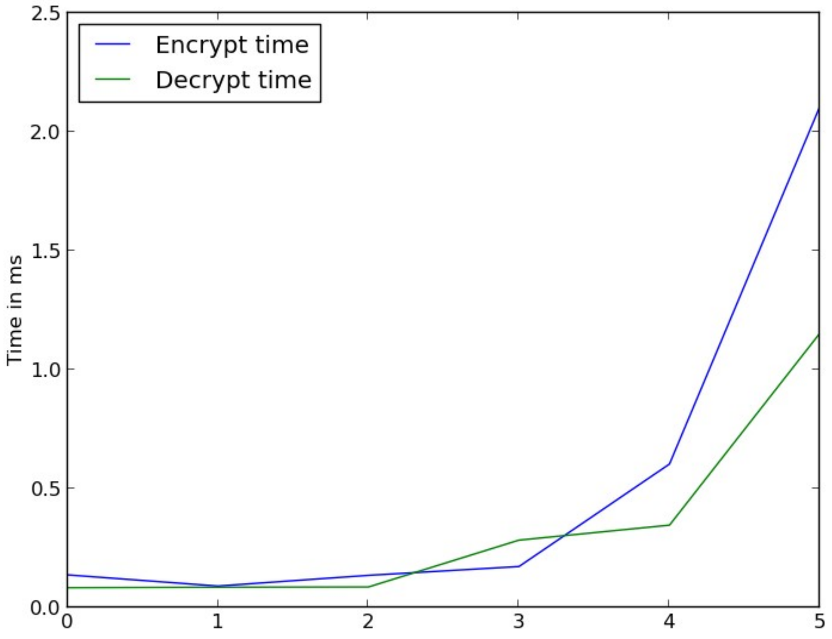
Figure 1. Diagram of Bitwise Hill Cipher

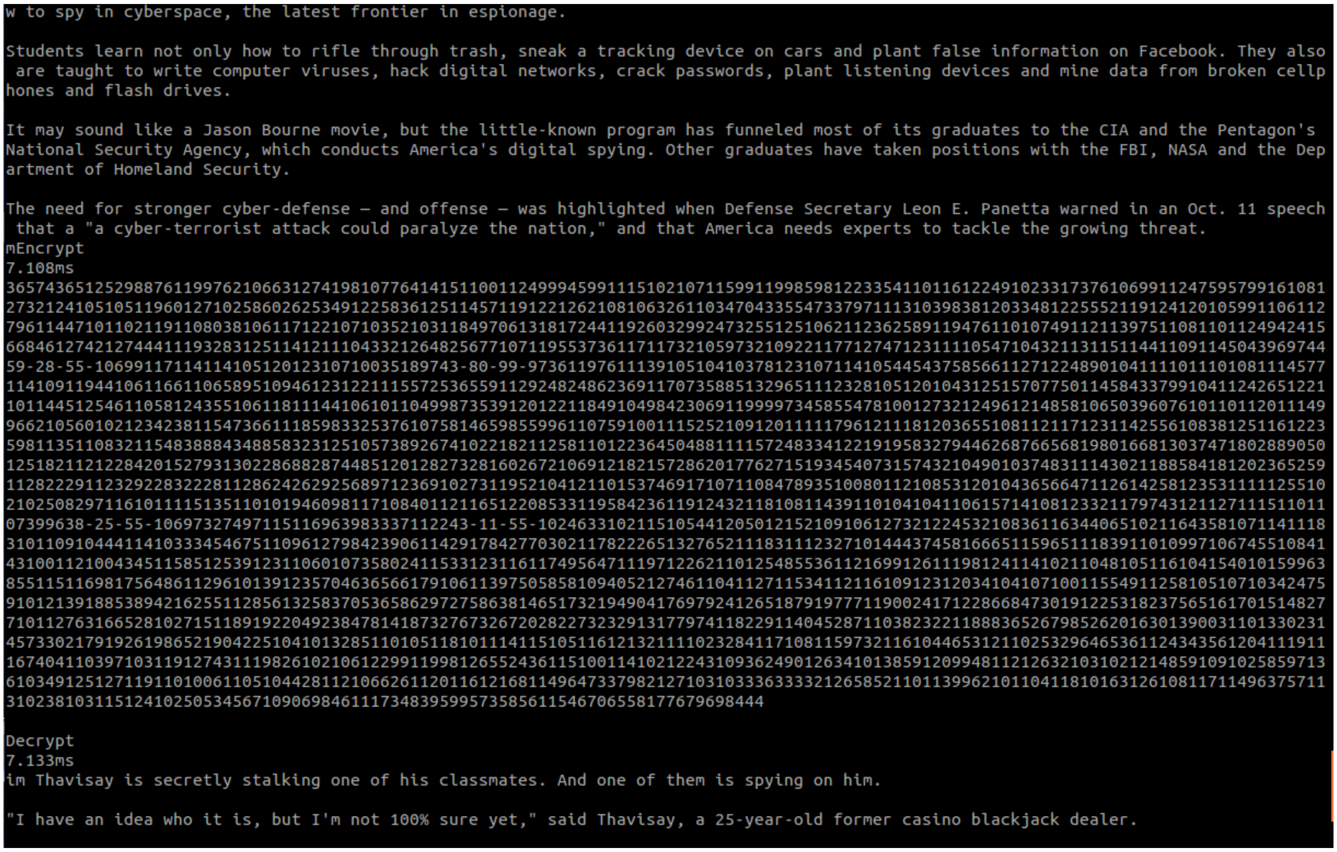
For the Cuda implementation, the file bytes will be read into a vector that is of the same size as the data to be stored, with the key being stored as another vector. These vectors are then multiplied using the matrixMul<<<>>>() fnuction that was used previously. It should be noted that the data is not being saved, due to the primary interest being the running time of the multiplication. Additionally, there are a lot of techniques that can be used to speed up this implementation.

Times for 2885 byte file:

Square Matrix Multiply
Encrypt 1.256ms
Decrypt 1.266ms
Encrypt 2.075ms
Decrypt 2.079ms
Encrypt 3.593ms
Decrypt 3.585ms
Encrypt 8.408ms
Decrypt 8.375ms
Encrypt 61.796ms
Decrypt 61.200ms
Encrypt 506.055ms
Decrypt 507.887ms

Cuda Times (encryption, decryption) are
Encrypt: 0.136ms
Decrypt: 0.082ms
Encrypt: 0.089ms
Decrypt: 0.084ms
Encrypt: 0.134ms
Decrypt: 0.085ms
Encrypt: 0.171ms
Decrypt: 0.282ms
Encrypt: 0.602ms
Decrypt: 0.345ms
Encrypt: 2.107ms
Decrypt:1.153ms





```
w to spy in cyberspace, the latest frontier in espionage.

Students learn not only how to rifle through trash, sneak a tracking device on cars and plant false information on Facebook. They also
 are taught to write computer viruses, hack digital networks, crack passwords, plant listening devices and mine data from broken cellp
hones and flash drives.

It may sound like a Jason Bourne movie, but the little-known program has funneled most of its graduates to the CIA and the Pentagon's
National Security Agency, which conducts America's digital spying. Other graduates have taken positions with the FBI, NASA and the Dep
artment of Homeland Security.

The need for stronger cyber-defense — and offense — was highlighted when Defense Secretary Leon E. Panetta warned in an Oct. 11 speech
 that a "a cyber-terrorist attack could paralyze the nation," and that America needs experts to tackle the growing threat.
mEncrypt
7.108ms
36574365125298876119976210663127419810776414151100112499945991115102107115991199859812233541101161224910233173761069911247595799161081
27321241051051196012710258602625349122583612511457119122126210810632611034704335547337971113103983812033481225552119124120105991106112
79611447101102119110803810611712210710352103118497061318172441192603299247325512510621123625891194761101074911211397511081101124942415
66846127421274441119328312511412111043321264825677107119553736117117321059732109221177127471231111054710432113115114411091145043969744
59-28-55-1069911711411410512012310710035189743-80-99-9736119761113910510410378123107114105445437585661127122489010411110111010811145 77
11410911944106116611065895109461231221115572536559112924824862369117073588513296511123281051201043125157077501145843379910411242651221
10114451254611058124355106118111441061011049987353912012211849104984230691199997345855478100127321249612148581065039607610110112011149
96621056010212342381154736611185983325376107581465985599611075910011115252109120111117961211181203655108112117123114255610838125116122 3
59811351108321154838884348858323125105738926741022182112581101223645048811115724833412219195832794462687665681980166813037471802889050
12518211212284201527931302286882874485120128273281602672106912182157286201776271519345407315743210490103748311143021188584181202365259
11282229112329228322281128624262925689712369102731195210412110153746917107110847893510080112108531201043656647112614258123531111125510
21025082971161011115135110101946098117108401121165122085331195842361191243211810811439110104104110615714108123321179743121127111511011
07399638-25-55-10697327497115116963983337112243-11-55-102463310211510544120501215210910612732122453210836116344065102116435810711411 18
31011091044411410333454675110961279842390611429178427703021178222651327652111831112327101444374581666511596511183911010997106745510841
43100112100434511585125391231106010735802411533123116117495647111971226211012548553611216991261119812411410211048105116104154010159963
85511511698175648611296101391235704636566179106113975058581094052127461104112711534112116109123120341041071001155491125810510710342475
91012139188538942162551128561325837053658629727586381465173219490417697924126518791977711900241712286684730191225318237565161701514827
71011276316652810271511891922049238478141873276732672028227323291317797411822911404528711038232211888365267985262016301390031101330231
45733021791926198652190422510410132851101051181011141151051161213211110232841171081159732116104465312110253296465361124343561204111911
16740411039710311912743111982610210612299119981265524361151001141021224310936249012634101385912099481121263210310212148591091025859713
61034912512711911010061105104428112106626112011612168114964733798212710310333633332126585211011399621011041181016312610811711496375711
31023810311512410250534567109069846111734839599573585611546706558177679698444

Decrypt
7.133ms
im Thavisay is secretly stalking one of his classmates. And one of them is spying on him.

"I have an idea who it is, but I'm not 100% sure yet," said Thavisay, a 25-year-old former casino blackjack dealer.
```

Figure 2. Example Encrypted/Decrypted Test