Lab #4

By: Brandi Durham, Andrew Miller

2.)

ROT - This is a cypher that allows an arbitrary rotation added to your plaintext message. Although this cipher isn’t used anymore because it has a max number of 26 combinations excluding special characters.

Vigenere - Change the value of a plaintext character with a new character based on a predetermined password.

Letter Numbers - Letters will be replaced with number, and letters with spaces.

Atbash - This is a simple character replacement cipher replacing the first character of the alphabet with the last IE: A->Z and so forth.

Playfair cipher - Uses a 5x5 matrix with one letter left out. You break up letters into pairs of two with repeated letters replaced with an x between them. Make a rectangle around the two letters, and the encrypted message is the opposite two corners.

3.)

Message 1: (Cracked with: A1Z26) (Letter Numbers)

Ciphertext: 1-20-20-1-3-11 1-20 4-1-23-14 23-9-20-8 4-18-15-14-5-19

Plaintext: A T T A C K A T D A W N W I T H D R O N E S

Message 2:

Ciphertext:

y. Tshoem eE yteo obfe Pervoivdiednecnec eo,f oar ctohnes pailrla-csye eiinnvgo levyien go ft hGeo df,o usnedeenr sh eorfe tohne tUhnei tUeSd $S1t abtielsl ,a nhda st hbee eInl ltuamkienna tbi

Plaintext: (Rotate cipher box length = 2 needs to be cleaned up a little)

.The Eye beProvidence, a the all-seeinglving the founders of on United$1 bill,   
hashe Illuminatiy some toof evidence oforconspiracy invoeye of God, seen herethethe US States and tbeen taken b

Message 3:

Ciphertext: (Caesarian Shift with n = 13)

Va zvq-1947, n Havgrq Fgngrf Nezl Nve Sbeprf onyybba penfurq ng n enapu arne Ebfjryy, Arj Zrkvpb.Sbyybjvat jvqr vavgvny vagrerfg va gur penfurq "sylvat qvfp", gur HF zvyvgnel fgngrq gung vg jnf zreryl n pbairagvbany jrngure onyybba.

Plaintext:

In mid-1947, a United States Army Air Forces balloon crashed at a ranch near Roswell, New Mexico.Following wide initial interest in the crashed "flying disc", the US military stated that it was merely a conventional weather balloon.

Message 4:

Ciphertext:

QW4gdW5pZGVudGlmaWVkIGZseWluZyBvYmplY3Qgb3IgVUZPLCBpcyBkZWZpbmVkIGFzIGEgcGVyY2VpdmVkIG9iamVjdCBpbiB0aGUgc2t5LCBub3QgaWRlbnRpZmlhYmxlIGJ5IHN0YW5kYXJkIGNyaXRlcmlhLiBNb3N0IFVGT3MgYXJlIGxhdGVyIGlkZW50aWZpZWQgYXMgY29udmVudGlvbmFsIG9iamVjdHMgb3IgcGhlbm9tZW5hLiBUaGUgdGVybSBpcyB3aWRlbHkgdXNlZCBmb3IgY2xhaW1lZCBvYnNlcnZhdGlvbnMgb2YgZXh0cmF0ZXJyZXN0cmlhbCBjcmFmdC4=

Plaintext: (base64 decoded after frequency analysis)

An unidentified flying object or UFO, is defined as a perceived object in the sky, not identifiable by standard criteria. Most UFOs are later identified as conventional objects or phenomena. The term is widely used for claimed observations of extraterrestrial craft.

Message 5:

Ciphertext:

Tn'tnhteotrdn a kr iur evoero yact lseen n, ncciaraaeefmo urZcpre 0s e7 sh sh.ahpweernoee mhhy ttleftg

Plaintext:

Part 2:

1. Ciphertext:

I #vT JLIKIXH KB IXDBLT YBV BD ?QMv X&ME KB NQOXHM BVL NVLL&XK NIWQ&L CYCKMT. I? QvOC NBTM KB vTY OKKMXKIBX KQ#K CBT& UMOLXME IXEIFIEVOUC NOvX ALMOR CVNQ CMNL&NY CNQ&TMC CITWUY AY KOAVUO?IXH N&LKOIX BNNVLL&XNMC BDv U&KKMLC, JQM?QML KQMY #L& MXNIWQML&E BL XBK. QBJ&FML, vI QOF& CBTM IEM#C KQOK JIUU OUUBJ VC ?B NBXKIXVM KB MZNQOXH& IXDBLTOKIBX JIKQBVK #XYBXM AMIXH OJOL& BD I?C T&OXIXH BL ITWBLKOXNM. Uv&? VvC TMMK #K KQ& MXE BD KvQM JMMR OK KQMv DBVXKOIX. I JIUU EMCNLIAM ?QM X&JUY EMFMUBWME NIWQML JQINQ KQMY COY IC NBTWU&?MUY VXALMOROAUM. VXKIU KQ&X, vEB XBvK KLVCK ?QIC NIWQ&L JIKQ #XY IXNLITIXOKIXH &FIE&XNM. KQM RIXH QvOC MYMC OXE M#LC MFMLYJQML&.

Plaintext: (cracked using substitution)

I #uM WRITING TO INFORM YOU OF ?HEu N&ED TO CHANGE OUR CURR&NT CIPH&R SYSTEM. I? HuAS COME TO uMY ATTENTION TH#T SOM& LEARNED INDIVIDUALS CAuN BREAK SUCH SECR&CY SCH&MES SIMPLY BY TABULA?ING C&RTAIN OCCURR&NCES OFu L&TTERS, WHE?HER THEY #R& ENCIPHER&D OR NOT. HOW&VER, uI HAV& SOME IDE#S THAT WILL ALLOW US ?O CONTINUE TO EXCHANG& INFORMATION WITHOUT #NYONE BEING AWAR& OF I?S M&ANING OR IMPORTANCE. Lu&? UuS MEET #T TH& END OF TuHE WEEK AT THEu FOUNTAIN. I WILL DESCRIBE ?HE N&WLY DEVELOPED CIPHER WHICH THEY SAY IS COMPL&?ELY UNBREAKABLE. UNTIL TH&N, uDO NOuT TRUST ?HIS CIPH&R WITH #NY INCRIMINATING &VID&NCE. THE KING HuAS EYES AND E#RS EVERYWHER&.

2) Ciphertext:

i r a d f e

r m w s a e

e e t x a p

e x

e o f o a t u t w t a t h b t t h e r w t

e y i x h n e d x e d l g x s o l e x

o e u n i d r e w o b m i c o a l u x r l

m a k s e t t n o o t n r s e e i o t n h

h o o

e a a t t p g r s t e u t u a c r r n t e

e d i e d a o t e w n i s a s n t i t r t

h o f e y u e t r v h t e i h n s e t m r

o e i f s n c s s

Plaintext: Couldn’t decrypt, but from the way the text in layout looks like it was encrypted using a block technique such as playfair or railfence.

Part 3)

1. RSA:
   1. “HI BOB” >> 8-9-28-2-15-2
   2. C = M^e mod n (encrypt)
   3. C = (89282152) ^ 47 mod 899
   4. C = 823
   5. Alice send 823 to Bob
   6. M = C^d mod n ( decrypt)
   7. M = 823^ 143 mod 899
   8. M = 664
2. You would have to win the lottery log367(2128) times