Exam 1 Funpack (Some solutions on last page)

1. Shift
   (a) Encrypt: 'cryptography is interchangeable with cryptology' by shift cipher where k=22
   (b) i. Decrypt: 'SOYYOUTHKGINOYGLATVRGIKZUROBK' where you know 'u " goes to 'A'
   ii. If you didn't know that u goes to A is there another way to decrypt this?
   (c) i. Decrypt: 'OCVJFTWPM' when you know 'on' goes to 'QP'.
   ii. since there are less letters what other way could you decrypt that does not involve frequency?

2. Affine Cipher
   (a) Is there an advantage to using a shift cipher followed by an affine cipher?
   (b) Encrypt: 'what is your favorite movie?" with $\alpha = 3$ and $\beta = 22$. Now decrypt to check.
   (c) Decode 'VYKRYNOLGBVNYLBLXCNNS' where you know 'is' goes to 'LX'.

3. Substitution: Decrypt the substitution cipher problems whose ciphertext is on the main class website (so that you can copy and paste into a computer program easily). The corresponding plaintext is given at the end of this document (so you can check your work, but won't be tempted to cheat :).

4. Vigenère: Decrypt the 3 messages on the main class website using a computer.

5. Playfair:
   (a) Using the key word 'algebra,' encrypt the plaintext 'geometry.'
   (b) Using the key word 'nevada,' encrypt the plaintext 'mississippi.'
   (c) Using the key word 'nevada,' decrypt the ciphertext 'AGHERYTOPIJXXD'
   (d) True or false: Two different plaintexts can be encrypted to the same ciphertext.

6. ADFGX / ADFGVX

(a)

	A	*D*	*F*	*G*	*X*
A	*g*	*a*	*z*	*b*	*y*
D	*h*	*I*	*f*	*c*	*r*
F	*d*	*w*	*e*	*v*	*k*
G	*u*	*l*	*p*	*m*	*q*
X	*t*	*x*	*s*	*n*	*o*

Keyword: math; Plaintext: caminofounders

(b)

	A	*D*	*F*	*G*	*X*
A	*z*	*d*	*I*	*o*	*s*
D	*e*	*y*	*c*	*u*	*p*
F	*l*	*f*	*x*	*b*	*k*
G	*q*	*m*	*g*	*w*	*a*
X	*t*	*r*	*n*	*h*	*v*

Keyword: teach; Plaintext: honeybeesting

(c)

	A	*D*	*F*	*G*	*V*	*X*
A	*a*	*l*	*u*	*j*	1	7
D	*m*	*b*	*k*	*t*	0	2
F	*v*	*n*	*c*	*I*	*s*	9
G	3	*w*	*o*	*d*	*h*	*r*
V	8	4	*x*	*p*	*e*	*g*
X	6	9	5	*z*	*q*	*f*

Keyword: heist; Plaintext: stealthemat930

7. Block and Hill
   (a) The plaintext 'friday' is encrypted using a Hill cipher with a 2x2 matrix. The ciphertext is 'HMUXWQ.' Find the encryption matrix.

(b) Find the inverse of $\begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix}$.

(c) The ciphertext 'GWQJZAWPBQLJ' was encrypted using the matrix $\begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix}$. Find the plaintext.

8. One time pads and Pseudo-random bit generation

   (a)

9. GCD, Euclidean Algorithm, solving $as + bt = \gcd(a, b)$

   (a) Using the euclidean algorithm, compute $\gcd(8125, 456)$. Check answer using Mathematica.

   (b) Solve $456x \equiv 3 \pmod{8125}$

   (c) Compute $\gcd(4883, 4369)$ and factor 4883 and 4369 into products of primes.

10. Multiplicative inverses mod n, inverting matrices mod n

    (a) Find the prime numbers less than 11 which make this matrix non invertible: $\begin{pmatrix} 3 & 8 & 1 \\ 2 & 5 & 6 \\ 4 & 9 & 7 \end{pmatrix}$ [Ans: 3,5]

    (b) Find the inverse of the previous matrix (mod 26).

    (c) Can the following matrix (mod 26) be invertible for any b? $\begin{pmatrix} 1 & 7 & 5 \\ 6 & 3 & 2 \\ 4 & 0 & b \end{pmatrix}$ [Ans: yes, for b=1]

    (d) Choose a value for b which makes the matrix (mod 26) non invertible, and show why. [Ans: 0 works. $\det(M) = -39b - 4$. $-4s - 26t \neq 1$]

11. Enigma problems

12. Feistel/DES problems

Substitution Cipher Solutions

1. hiihopeyouhaveenjoyedsolvingthisproblembymejonnykimyouprobablydidnotenjoy solvingthisproblemasmuchasihaveenjoyedmakingthisproblemforyouitissoeasytoma keasubstitutionproblembecauseallineedtodoisjusttypeonaworddocumentthenuseth efindandreplacetooltohowevernowthatiamthinkingaboutitimnotsurehowimgoingto dothissinceificonvertalettertoadifferentletterthenwhenitcomestimetoconvertthelett erijustconvertedtoiwillbeconvertingletterssthatarealreadyconvertedwelliguessilljust havetobealittlemoreorganizedwheniconverteachletterperhapsamoresystematicappr oachwillsufficeanywaysgoodluckonthetesttomorrow

2. wowifyouarereadingthisandhavecompletedproblemnumberonetheniamimpressed wellmaybeyoureallylikesubstitutioncipherproblemsbutipersonallythinkthatyourtim ewillbebetterspentstudyingtheoremsandothercipherproblemslikethehillcipherorth eaffinecipherortheengimaoreventheplayfairandthegermanafgxsomethingorotherma nthosegermansarereallysneakyhuhprettysmartforthemtocomeupwithsuchaniftycip hermachineliketheenigmaohbythewaychurchhilldidntsaythatcrackingtheenigmacut twoyearsoffthewarwhathedidsaywastothecurrentkingofenglandkinggeorgethesixtht hatcrackingtheenigmawonthewarthatisaprettyboldstatementimeaniknowiwasntthe reandallbutithinkthegermanswouldhaveeventuallylostimeancmontheywerefighting onmultiplefrontsagainstustheyanksthebritsandeventherussianswelliwillstopbabblin gihopethisproblemhashelpedyou

3. oksothisisthelastproblemimnotsurewhatkindofmessageishouldcreateforthethirdpro blemsothefirstproblemiactuallywentthroughthemeticulousprocessofsubstitutingea chletterforadifferentoneletmetellyouthatwasnotfunthenforthesecondproblemisaidt omyselftherehasgottobeabetterwaytodothissoaquickcursorysearchongoogleyielded theresultsiwaslookingforifoundawebsitehttptwentyfiveyearsofprogrammingcomfor wardslashfunforwardslashcipherssthatgavemetheoptiontopastemyplaintextinoneblo ckthenhitabuttonandbamgetthecipherttextwowthatwassomucheasierthanthepainsta kingprocessididwiththefindandreplacefunctiononwordalrightitsgettinglatenowand iwouldliketostudyorgotosleeporplayplantsandzombiesonmyphonesoiamendingthis messagenowihopethismessageislongenoughforsomeonetoperformanaccuratefreque ncycountgoodluckonthetest