Summary of Topics

1. Cryptography

   - Know how to encrypt and decrypt a message using
     - a Caesar cipher
     - an alpha-numeric cipher given a substitution mapping
     - a transposition cipher given the length of a row
     - a transposition cipher given an encryption keyword
     - a shifting substitution cipher
     - a Vigenére cipher
     - a double transposition cipher
   - Know how to use letter frequency to decrypt a message without an encryption key.
   - Know which encryption methods do or do not preserve letter frequency.
   - Be able to articulate strengths and weakness in each of the encryption methods learned.

2. Finance
   You will be given the formulas below. For each calculation, you should be able to calculate the correct answer and be able to correctly **write down the calculation you used to obtain the correct answer**.

   Formulas

   $$A = P + I \qquad A = P(1+rt) \qquad A = P\left(1+\frac{r}{n}\right)^{(nt)} \qquad P = \frac{A}{\left(1+\frac{r}{n}\right)^{(nt)}}$$

   $$P = \frac{d(1-\left(1+\frac{r}{n}\right)^{(-nt)}}{\left(\frac{r}{n}\right)} \qquad d = \frac{A\left(\frac{r}{n}\right)}{\left(1-\left(1+\frac{r}{n}\right)^{(-nt)}\right)}$$

   - Calculate tip on a bill.
   - Know the terminology and notation of principal (P), interest (I), annual interest rate (r), compounding frequency (n), time (t), payment amount (d), and future value (A).
   - Distinguish between simple interest and compound interest.
   - Distinguish between an annual interest rate (APR) compounded at some rate and the effective annual interest rate (EAR).
   - Calculate the future value, A, and interest, I, over a period of time in a savings account or loan given that the interest is simple or compounded at a given rate.
   - Calculate the principle, P, required to obtain a given future value on a savings or loan account given the time period, annual interest rate and compounding rate.
   - Determine the monthly payment on a loan of a given amount at a given rate and time and then the total amount paid for the loan.

Sample Problems

1. Encrypt the message GO TO BERLIN using

   (a) a Caesar cipher with a shift of 24 (A to Y)

   G O T O BERLIN
   F M R M ZCPJGL

   (b) a transposition cipher given a row length of 5.

   G O T O B
   E R L I N

   cipher text : GEORTLOIBN

   (c) a transposition cipher given encryption keyword STOP.

   S T O P
   G O T O
   B E R L
   I N

   O P S T
   T O G O
   R L B E
   I N

   Cipher text : TROLGBIOEN

   (d) a shifting substitution cipher starting with a shift of 6 (A to G).

   6 7 8 9 10 11 12 13 14 15
   G O T O B E R L I N
   M H B X L P D Y W C ← cipher text

   (e) a Vigenére cipher with key word STOP.

   S T O P S T O P S T
   G O T O B E R L I N
   Y H H D T X F A A G ← cipher text

   (f) a double transposition cipher with first key word BLUE and second key word GOLD.

   BLUE
   GOTO
   BERL
   IN

   BELU
   GOOT
   BLER
   I N

   rewrite by columns
   GBIOLOENTR

   GOLD
   G B I O
   L O E N
   T R

   DGLO
   O G I B
   N L E O
   T R

   encrypted text : ONGLTIEBOR

2. Using the alpha-numeric substitution below to answer the questions.

original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
maps to	9	8	7	6	5	4	3	2	1	0	D	C	B	A	H	G	F	E

original	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9
maps to	L	K	J	I	P	O	N	M	T	S	Q	R	V	U	Y	X	W	Z

   (a) Encrypt the plain text RIGHT 10 LEFT 25

   R I G H T 1 0 L E F T 2 5
   E 1 3 2 K S T C 5 4 K Q U ← encrypted text

   (b) Decrypt the encrypted text K5OKTTQXW

   K 5 O K T T Q X W
   T E X T Ø Ø 2 7 8 ← decrypted text

3. Decrypt each encrypted text using the specified mechanism.

   (a) cipher text: NJCYQC,
   encryption mechanism: a Caesar cipher with a shift of 24 (A to Y)

   N J C Y Q C
   P L E A S E ← message

   (b) cipher text: DFTOO ANRBO GCTED, ← 15/5 = 3 col. length
   encryption mechanism: a transposition cipher given a row length of 5

   D O N O T
   F O R G E
   I A B C D

   message: Do NOT FORGET ~~ABCD~~

   (c) cipher text: DMFAT 3RYME IIIRSD, encryption mechanism: a transposition cipher given encryption keyword STOP

   16 letters. 16/4 = 4

   O P S T
   D T M I
   M 3 E R
   F R I S
   A Y I D

   S T O P
   M I D T
   E R M 3
   I S F R
   I D A Y

   message:
   MIDTERM 3 IS
   FRIDAY

   (d) cipher text: HYQWQ,
   encryption mechanism: a shifting substitution cipher starting with a shift of 6 (A to G)

   6 7 8 9 10
   H Y Q W Q
   B R I N G

   message: Bring

   (e) cipher text: FHHTK ASTL,
   encryption mechanism: a Vigenére cipher with key word STOP

   S T O P S T O P S
   F H H T K A S T L
   N O T E S T E E T

   message: notesheet

   (f) cipher text: OEAOM NTSLD, ← 10 letters.
   encryption mechanism: a double transposition cipher with first key word BLUE and second key word GOLD.

   D G L O
   O A N S
   E O T L
   M D

   G O L D
   A S N O
   O L T E
   M D

   extracted rows: ASNOOLTEMD

   B E L U
   A O L M
   S O T D
   N E

   B L U E
   A L M O
   S T D O
   N E

   extract rows:
   ALMOST
   DONE

4. Which of the encryption methods in problems 1 and 2 above preserve letter frequency?
   - Caesar shift.
   - transposition ciphers of any kind.

5. Pikachu takes out a simple interest loan of \$500 with an annual interest rate of 6.24%. Suppose Pikachu repays the loan in 2 years and 4 months later.

   (a) How much did Pikachu pay?

   $P = \$500$ $t = 2.33$ $r = 0.0624$

   $A = P(1+rt) = 500(1+0.0624(2.33)) = \$572.70$

   (b) How much of the payment was interest?

   $I = A - P = 572.70 - 500 = \$72.70$

6. Charizard invests in a certificate of deposit that offers 4.2% APR compounded daily.

   (a) If Charizard invests \$1000, how much will be in the account in 10 years and what percentage of the total is the accumulated interest? (We are supposing no additional investments or withdrawals over the 10 years.)

   $P = \$1000$ $n = 365$ $r = 0.042$ $t = 10$

   $A = P\left(1+\frac{r}{n}\right)^{nt} = 1000\left(1+\frac{0.042}{365}\right)^{365\cdot 10} = \$1521.92$ ← total

   $I = 1521.92 - 1000 = 521.92$

   (b) What is the effective annual interest rate (EAR) of this investment?

   Choose $P = \$100$, $r = 0.042$, $n = 365$, $t = 1$

   $A = 100\left(1+\frac{0.042}{365}\right)^{365} = 104.29\ldots$ So 4.29%

   (c) How much would Charizard need to invest in order for the account to contain \$10,000 at the end of 20 years?

   Use: $P = \frac{A}{\left(1+\frac{r}{n}\right)^{(nt)}} = \frac{10{,}000}{\left(1+\frac{0.042}{365}\right)^{365(20)}} = \$4{,}317.31$

7. Mewtwo takes out a 15 year mortgage for \$150,000 at 5.8% APR compounded monthly.

   (a) What is Mewtwo's monthy payment? (Find d.)

   Use $d = \frac{P\left(\frac{r}{n}\right)}{\left(1-\left(1+\frac{r}{n}\right)^{(-nt)}\right)} = \frac{(150000)\left(\frac{.058}{12}\right)}{\left(1-\left(1+\frac{0.058}{12}\right)^{-(15)(12)}\right)} = \$1249.63$

   (b) How much is Mewtwo paying over the life of the mortage?

   $\$1249.63 \cdot 15 \cdot 12 = \$224{,}933.40$

   (c) Suppose Mewtwo is unwilling to have a monthly payment of more than \$800 per month. How large mortgage is possible assuming the same APR and monthly compounding?

   Use $P = \frac{d\left(1-\left(1+\frac{r}{n}\right)^{(-nt)}\right)}{\left(\frac{r}{n}\right)} = \frac{800\left(1-\left(1+\frac{0.058}{12}\right)^{-12(15)}\right)}{\frac{0.058}{12}} = \$96{,}028.06$