Question 1.

Decrypt the following cryptotexts:

(a) The given ciphered text is encoded using Bacon's cipher.

From `AAAAB AAAAA AAABA ABBBA ABBAB AAABA ABAAA ABBBB AABBB AABAA BAAAB`, we obtain `BACONCIPHER`.

(b) The given ciphered text is a anagram. There are more possible ways how to decode the given text. For example `LESTER SANDERS HILL` or`HANDLIST RESELLERS`.

(c) The given ciphered word is encoded using Four Square cipher.

We obtain `ITWASINVENTEDBYFELIXDELASTELLE` after decoding the given ciphered word using the Four Square decoding algorithm with keys being `four` and `square`.

Question 2.

(a) $e_{7,19}(A) = (A.7 + 19) \bmod 26 = (0.7 + 19) \bmod 26 = 19 \bmod 26 = 19 = T$

$e_{7,19}(F) = (F.7 + 19) \bmod 26 = (5.7 + 19) \bmod 26 = 54 \bmod 26 = 2 = C$

$e_{7,19}(I) = (I.7 + 19) \bmod 26 = (8.7 + 19) \bmod 26 = 75 \bmod 26 = 23 = X$

$e_{7,19}(N) = (N.7 + 19) \bmod 26 = (13.7 + 19) \bmod 26 = 110 \bmod 26 = 6 = G$

$e_{7,19}(E) = (E.7 + 19) \bmod 26 = (4.7 + 19) \bmod 26 = 47 \bmod 26 = 21 = V$

Ciphertexxt = `TCCXGV`

(b) $7^{-1} \bmod 26 = 15$

$d_{7,19} = (15.(H - 19)) \bmod 26 = (15.(7 - 19)) \bmod 26 = 2 = C$

$d_{7,19} = (15.(T - 19)) \bmod 26 = (15.(19 - 19)) \bmod 26 = 0 = A$

$d_{7,19} = (15.(V - 19)) \bmod 26 = (15.(21 - 19)) \bmod 26 = 4 = E$

$d_{7,19} = (15.(P - 19)) \bmod 26 = (15.(15 - 19)) \bmod 26 = 18 = S$

$d_{7,19} = (15.(I - 19)) \bmod 26 = (15.(8 - 19)) \bmod 26 = 17 = R$

Plaintext = `CAESAR`

Question 3.

(3 points) What is the number of possible keys and the unicity distance of an affine cipher if the following modulus is used:

For a modulus of 26, the number of possible keys is

$n = \varphi(26) \cdot 26 = 12 \cdot 26 = 312,$

where φ is the Euler's totient function, as we can have $\varphi(26)$ different values of a co-prime to 26 and 26 different values of b.

1. 30

   $n = \varphi(30) \cdot 30 = 8 \cdot 30 = 240$

   $U = \frac{H_K}{D_L} = \lceil \frac{\log 240}{3.2} \rceil \doteq \lceil 2.47 \rceil = 3$

   The number of possible keys is 240, the unicity distance is 3.

2. 31

   $n = \varphi(31) \cdot 31 = 30 \cdot 31 = 930$

   $U = \frac{H_K}{D_L} = \lceil \frac{\log 930}{3.2} \rceil \doteq \lceil 3.08 \rceil = 4$

   The number of possible keys is 930, the unicity distance is 4.

Question 4.

(a)

i. Since the keyspace is basically the set of possible values of a, it always holds that $|K| = n-1$, because $0 \notin K$. That implies that $|K| < |M|$, which means that this encryption function is not perfectly secure. It's also obvious that $Pr[P = 0|C = 0] = 1$ (zero always gets encrypted as zero) and assuming that $n > 1$, $Pr[P = 0] \neq 1$, therefore $Pr[P = 0|C = 0] \neq Pr[P = 0]$.

ii. Since the keys (b) are uniformly distributed and $|K| = n$, $Pr[K = b] = \frac{1}{n}$.
$Pr[C = c] = \frac{1}{n}$, because $c = x + b\,(mod\,n)$, x and b are independent and b is uniformly distributed:

$$\sum_{b\in\mathbb{Z}_n} P[X = c - b\,(mod\,n)] = \sum_{x\in\mathbb{Z}_n} P[X = x] = 1.$$

$$Pr[C = c|P = x] = Pr[K \equiv c - x\,(mod\,n)] = \frac{1}{n}.$$

$$Pr[P = x|C = c] = \frac{Pr[P=x]\cdot\frac{1}{n}}{\frac{1}{n}} = Pr[P = x]$$

This means that it is a perfectly secure cryptosystem.

iii. Here the key consists of a and b ($k =$), therefore $|K| = n(n-1)$ and assuming the keys are used with equal probability, $Pr[K = k] = \frac{1}{n(n-1)}$.
Since n is a prime and $a, b < n$, it holds for every a that $gcd(a, n) = 1$ and $gcd(b, n) = 1$. This means that there are no two different keys (combinations of a, b), that encrypt message x to the same c. Therefore:

$$Pr[C = c] = \sum_{i\in P} Pr[P = i] \cdot \sum_{k:e_k(i)=c} Pr[K = k] = 1 \cdot Pr[K = k] = \frac{1}{n(n-1)}$$

$$Pr[C = c|P = p] = \sum_{k:e_k(p)=c} Pr[K = k] = Pr[K = k|e_k(p) = c] = \frac{1}{n(n-1)}$$

$Pr[C = c] = Pr[C = c|P = p] = \frac{1}{n(n-1)}$, so this is also a perfectly secure cryptosystem.

(b) The smallest number of encryption functions must be $|K| \geq n$ (and the encryption functions must be chosen uniformly), so there would be equal probability that any plaintext message p will be encrypted to any c, in other words, we need enough encryption functions so that any plaintext message p can get encrypted to any ciphertext message c. If we had less than n encryption functions, some of the ciphertext messages c would occur with higher probability.

Question 5.

(a) We have :

$$c_1 = w_1 \oplus w_2 \oplus w_3 \oplus k,$$
$$c_2 = w_2 \oplus w_3 \oplus k,$$
$$c_3 = w_3 \oplus k$$

Taking the XOR of c_1 and c_2 we get $c_1 \oplus c_2 = w_1 \oplus w_2 \oplus w_3 \oplus k \oplus w_2 \oplus w_3 \oplus k = w_1$.
Also taking the XOR of c_2 and c_3 we get $c_2 \oplus c_3 = w_2 \oplus w_3 \oplus k \oplus w_3 \oplus k = w_2$.

Therefore Bob can recover the messages in the following way:

$$w_1 = c_1 \oplus c_2,$$
$$w_2 = c_2 \oplus c_3,$$
$$w_3 = c_3 \oplus k$$

(b) Malicious Eve can discover the length n of the messages and of the key respectively.
She can also recover the binary messages w_1 and w_2 using the above mentioned procedure.

Question 6.

UACVL	GVWUN	CVETM	QUCGT	RPMAO	UWYJM	UHFMH	FPTGV	RGKEV	IQBPR	NEUIR	HBBVW	YRGJB	EOEEC
YEZKJ	MEXNG	CQTPJ	QNRLO	PHLFK	ITAIL	SQUEW	ZXJMH	PAJNP	SSYVA	ILDJM	NOMIT	RWXNU	WZMGP
GMEEY	VHCET	SIGIS	EEVPC	RYUXH	XNFPP	RGYDE	ILHFX	TTKLG	WILCP	PPRPG	CFEMO	MCRHK	SPEYB
NUBPT	NIPMI	XTIWP	NKYTR	WAEOM	NHFPC	KSXXB	GTNVH	DTBUA	HYDEO	XGGSB	VFHZT	VWKGT	AENYL
NKMOX	HBSUY	NHEMS	NEPAT	CYDVT	GGDXN	UFJDZ	WEHVX	RFXMY	WVKXD	KIDBH	ICLGE	MDATC	DKZET
XTBRF	XZFWM	EXRBN	UBPPI	YULIT	NBLXY	VZGKS	BNDYH	HVRJX	PNBMC	DHVHJ	BSVRZ	JEAEE	NRTBC
CLPAB	XJKON	GICYD	ZIIXH	XINMN	HIMHM	EGUOX	OIVHG	VHBFG	LTRBY	PLTLE	DLPTN	VKMIG	GBHOT
YICKT	HFEYN	IGLGK	IGGUB	PTVGJ	GIJUF	BLSSI	GGKGO	XHLSK	LGDAL	ITETT	VWVTN	WBBVM	AXIUV
OGTSC	MUKMQ	GHTSC	YPNCE	TZEEY	JAYOI	IFTNW	WISOI	UFCUB	TGFZL	ICXQI	UULJW	TZVLK	LCKAD
ETNXS	HLUVH	BPTTR	PEBPA	ESBPC	VVVTI	GLZBL	DRLCU	IMOGH	ZTWMP	BSAIO	AARFN	GVTLA	OXYOK
TWULB	SICYG	YMUWI	LCPPP	RZIUP	HBCIG	TGYXU	NGZET	NEHRX	VAILI	TDFSK	SPXMH	RFYIA	DTNXO
YHJMW	ATOCW	ABSJW	LLRXV	BTNDF	BZWVZ	GKTAE	SYTSR	RCETX	ROUEI	MIGQP	EAOUE	IFRJB	SWITW
ZVVVA	HCVUS	LPDJS	QGAYT	FLEHV	SWMBK	EBEZF	KLGVR	BMFUY	WRVCG	DHNFN	SEFVA	BSMHB	NTTXE
XXTAE	CLTTZ	WJTCE	EBLLD	MEPMA	ZEPPP	RKLGB	RKUTM	TAEIP	XMRIU	CDQLM	VXPHS	TCMLV	XJTTU
RJNTS	YMPME	ELJAP	NTIFX	MTNEY	OTYEV	UAUBB	APKVI	RAILW	PLVSV	GTXTM	HVMAR	FZKWI	GGUBP
MNMVA	AGIOY	JERVJ	XAWSU	UCTFZ	GKTAE	SYDTF	JVAEP	OSFOI	WXJBS	PATNS	ETEUX	TAEOC	EWFYN
WFBTJ	HHIKL	VAEEO	OADTR	RFBNZ	TSUOI	KMQGO	YHVMS	IEKWI	CHDFV	CEROK	GGTCI	CPVVQ	GGTLI
ONSEZ	RVXRX	SUMZF	EEVBO	GAMMP	CLVKM	YTPSU	NTZGG	MHTTI	UDCFR	VBNNE	ECYTF	XJXTP	EONTE
KLEXN	MUSSD	IDSPL	IGGIN	SETSF	XBHOL								

This is KASISKI method:

substring	distances of occurences	distance
TAE	gcd([528, 638, 676, 803, 836]) =	1
IGG	gcd([22, 41, 561, 792]) =	1
AIL	gcd([22, 649, 924]) =	11
PPR	gcd([22, 550, 770]) =	22
KLG	gcd([352, 693, 759]) =	11
UBP	gcd([154, 297, 836]) =	11

GCD of found distances is 11, I'm going to try this length and compute corresponding indices of correspondence:

```python
# This is algorithm how I obtain 11 columns below
for column in range(0, 11):
    print( column )
    for i in range(len( cryptotext ) ):
        if i % 11 == column:
            print(cryptotext[i])
```

1. UVMMVHOXLLPLXESXLLMBXAXUBABPXXKDBBTBNVBNXGBLGHGJGLWGTEWTUKV AGMALBLBZLHYBNAXEWVYKBHMAEZKRHUETULMGGWAPPABEZYHTLXGTTNPMGH

2. AEAHIBENOSADNYENHCONTEXAVESANRIARNNNBRCGIUFEGFGUOIBTSYWGLAHE LOIASCCEIRHSDERAIUTEMNHEEEUISRLNBWHGISEOAETOTHDCISAPTEEUGO

3. CTOFQBEGPQJJUVEFFPMUIOBHFNUTUFDTFUBDMZCINOGDBEUFXTBSCJIFJDB SZGOOIPITTFJJFSOOTSFBFFBCBPTUTJJEBPVUOUSSTOJOSVFIOUMSIEOSIL

4. VMUPBVCCHUNMWHVPXPCBWMGYHYYCFXBCXBLYCJLCMXLLHYBBHEVCYASZWEP BBHAXCPGNDYMWBYUUWLLEUNNLLPMCCNAYALMBYUYFNCHAUMVCNMMUUCNSN

5. LQWTPWYQLEPNZCPPTPRPPNTDZLNYJMHDZPXHDEPYNOTPONPLLTMMPYOLTTT PLZAYYPTEFIWLZTEEZPEZYSTTLPTDMTPOPVAPJCDOSEHDOSCPSZPNDYTDS

6. GUYGRYETFWSOMECRTRHTNHNETNHDDYIKFPYHHAADHIRTTITSSTAUNOIIZNT
CDTROGRGHSAALWSIIVDHFWETTDRAQLSNTKSRMETTIEWITIIEVEFCTCTEIE
7. VCJVNRZPKZSMGTRGKPKNKFVOVKEVZWCZWIVVVEBZIVBNYGVSKVXKCIUCVXR
VRWFKYZYRKDTRVRMFVJVKRFXZMKELVYTYVVFNRFFWTFKRKERVZELZFFKDT
8. WGMREGKJIXYIPSYYLGSIYPHXWMMTWVLEMYZRHEXIMHYVILGILWIMEIFXLSP
VLMNTMIXXSTOXZRIRVSSLVVEWELIMXMIEIGZMVZJXEYLRMKOQREVGRXLSS
9. UTUGUJJQTJVTGIUDGCPPTCDGKOSGEKGTEUGJJNJIHGPKCGJGGVUQTFCQKHE
VCPGWUUUVPNCVGCGJAQWGCAXJPGPVJPFVRTKVJGVJUNVFQWKGVVKGVJEPF
10. NRHKIBMNAMARMGXEWFEMRKTGGXNGHXEXXLKXBRKXMVLMKKGGDTVGZTUILLB
TUBVUWPNAXXWBKEQBHGMVGBXTMBXXTMXUAXWAXKABXWABGIGGXBMMBXXLX
11. CPFEREERIHIWEIHIIEYIWSBSTHEDVDMTRISPSTOHEHTITIIKANOHENBUCUP
IISTLIHGIMOATTTPSCABRDSTCARMPTEMAITIAATESTFENOCGTROYHNTNIB

Collumn	Index of correspondence
1	0.05708
2	0.06244
3	0.06316
4	0.06278
5	0.07574
6	0.06248
7	0.07118
8	0.06057
9	0.07515
10	0.07324
11	0.06823

Indices of correspondence are high, thus the key length is 11. All columns are encoded with Caesar cipher. We can use frequency analysis, where "E" most used letter in English and Vigenère table to decode. If "E" doesn't make sense, try other widely used letter.

Collumn	Most frequent letters	Corresponding row in Vigenère table
1	B,X,L	Y,T,H
2	E	A
3	F	B
4	Y, C	U,X
5	P	L
6	I, E, T	E,A,P
7	V	R
8	I	E
9	G	C
10	X	T
11	I, E, T	E,A,P

BABBAGES SUCCESSFUL CRYPTANALYSIS OF THE VIGENERE CIPHER WAS PROBABLY ... ACHI EVEDINEIGH TEENF IFTYF OURSO ONAFTERHIS SPATW ITHTH WAITE SBUTH ISDIS COVER YWENT COMPLETELY UNREC OGNIZ EDBEC AUSEH ENEVE RPUBL ISHED ITTHE DISCO VERYC AMETO LIGHT ONLYINTHET WENTI ETHCE NTURY WHENS CHOLA RSEXA MINED BABBA GESEX TENSI VENOT ESINT HEMEANTIME HISTE CHNIQ UEWAS INDEP ENDEN TLYDI SCOVE REDBY FRIED RICHW ILHEL MKASI SKIARETIRE DOFFI CERIN THEPR USSIA NARMY EVERS INCEW HENHE PUBLI SHEDH ISCRY PTANA LYTICBREAK THROU GHIND IEGEH EIMSC HRIFT ENUND DIEDE CHIFF RIRKU NSTSE CRETW RITIN GANDTHEART OFDEC IPHER INGTH ETECH NIQUEHASBE ENKNO WNAST HEKAS ISKIT ESTAN DBABB AGESCONTRI BUTIO NHASB EENLA RGELY IGNOR EDAND WHYDI DBABB AGEFA ILTOP UBLIC IZEHI SCRACKINGO FSUCH AVITA LCIPH ERHEC ERTAI NLYHA DAHAB ITOFN OTFIN ISHIN GPROJ ECTSA NDNOTPUBLI SHING HISDI SCOVE RIESW HICHM IGHTS UGGES TTHAT THISI SJUST ONEMO REEXA MPLEOFHISL ACKAD AISIC ALATT ITUDE HOWEV ERTHE REISA NALTE RNATI VEEXP LANAT IONHI SDISCOVERY OCCUR REDSO ONAFT ERTHE OUTBR EAKOF THECR IMEAN WARAN DONET HEORY ISTHA TITGAVETHE BRITI SHACL EARAD VANTA GEOVE RTHEI RRUSS IANEN EMYIT ISQUI TEPOS SIBLE THATBRITIS HINTE LLIGE NCEDE MANDE DTHAT BABBA GEKEE PHISW ORKSE CRETT HUSPR OVIDI NGTHEMWITH ANINE YEARH EADST ARTOV ERTHE RESTO FTHEW ORLDI FTHIS WASTH ECASE THENI TWOULDFITI NWITH THELO NGSTA NDING TRADI TIONO FHUSH INGUP CODEB REAKI NGACH IEVEM ENTSINTHEI NTERE STSOF NATIO NALSE CURIT YAPRA CTICE THATH ASCON TINUE DINTO THETW ENTIETHCEN TURYS IMONS INGHT HECOD EBOOK