Task 1

The words which we know from the corresponding plaintext:

(a) Technique
(b) Significant
(c) Compared
(d) Operate

We have to find the upper matrix

The digram mappings that can be discovered are following

TECHNIUE

EC → CB
HN → NH
IU → BP

SIGNIFICANT

SI → UF
GN → HM
IF → FI
IC → YA
AN → NA

COMPARED

CO → RM
MP → KS
AR → TT
ED → UB

OPERATE

PE → ZA
RA → SE
TE → BB

The given lower Matrix is:

a b c d e
F g h i J
K L M N O
P R S T U
V W X Y Z

First We'll Form the Matrix For:

(1) TECHNIUE

I _ _ _ B
_ _ _ _ _
_ _ _ _ _
_ e c _ _
_ _ _ H _

EC → CB
HN → NH
IU → BP

a b c d e
F g h i J
K L M N O
P R S T U
V W X Y Z

(2) COMPARED

_ e _ U _
K _ M _ _
_ _ _ _ _
_ t _ A _
_ _ c _ R

CO → RM
MP → KS
AR → TT
ED → UB

a b c d e
F g h I J
K L M N O
P R S T U
V W X Y Z

(3)

(3) SIGNIFICANT

```
_ _ _ a _
_ _ G H _
I _ Y _ _
S _ _ U _
I _ _ _ _
```

SI → UF
GN → HM
IF → FI
IC → YA
AN → NA

```
a b c d e
F g h I J
K L M N O
P R S T U
V W X Y Z
```

(4) OPERATE

```
_ _ _ _ _
P _ _ _ Z
_ _ _ _ _
S _ _ _ R
_ T _ _ B
```

PE → ZA
RA → SE
TE → BB

```
a b c d e
F g h I J
K L M N O
P R S T U
V W X Y Z
```

(4)

Description # We form the matrix by marking the 2nd letter from 1st pair and 2nd letter from the 2nd pair in the lower matrix. After we've marked, in the same column but in any row of the empty matrix we'll write the corresponding letters of the mapping. For eg if we have mapping

SI → DF

We'll mark I & F in the lower matrix, then in the same columns of the empty matrix we'll write S for F and I for E such that it forms a square.

Now after forming, we'll join all the upper matrix in such a way that we dont repeat any word in the columns.

My Final Matrix after Joining is:

P	_	G	H	Z
I	t	Y	a	b
S	E	C	U	R
K	_	M	_	_

If we observe we'll see that our keyword is "SECURITY" which is present in the 3rd & 4th row so, we can form the Final upper matrix

S	E	C	U	R
I	T	Y	A	B
D	F	G	H	J
K	L	M	N	O
P	V	W	X	Z

For finding, plain text From our ciphertext we needed upper matrix with the keyword and the lower matrix which was already given

S E C U R
I T Y A B
D F G H J
K L M N O
P V W X Z

A B C D E
F G H I J
K L M N O
P R S T U
V W X Y Z

So, the plain text recovered after following all the techniques written on wikipedia page we have:

thetecmiiueencryptwpiars of lettre
ythkthusFallsiaïloacategoryofciph
rempnown aspolygrapyFcaubstitbrio
nc xFhersthis dadssignhgickdtsrven
gtgo the encryption Fyen comparedwi
th monograpyFcaubstitbrion cxFhers
Fyichoperate on single gdoracters.

If we arange all the wods we'll yet

"
The technique encrypts pairs of letters and thus falls into a category of ciphers known as polygraphic substitution ciphers. this adds significant strength to the encryption when compared with monographic substitution ciphers which operate on single characters."