Homework 02

Solutions

Question 1

Guess Key Length

In[93]:=
```
ciphertext = StringSplit[
    "AWQEIWLADIGTVPMNRBQKEEDGVYEQTIDZNUMTEQPKBJPGVSTAVIRZVVLEMIPOAYLQJHLDKRGYWVLI↖
       YOVSDZWPGEZZVAINMULESIFTEPXGHIYBQXHPJQSKSMTWIDBGVWLATIAOQPKBFBKXHLLPSPT↖
       KVYRPAQVCZVXIRDIVMOYAKRIEIPHWSIVMSEPGYSPWHEBZWMXHZCILTLTKGEHQVLOFBRMCEC↖
       TISZZESNGMTWAEQQRSZAJIWLAESNDQFIRTVIMNSMTSWYUKRDLAYILWIUWHPKQYLONQVTSMJ↖
       STOIAQAOMJIRQMGPVPZAWLPMRCAYLUXUAQFAHPBJIREPGTLPIUYRPWHQAVQPKAOIKWYNPCM↖
       NHWWPDMMYSREPVLEEZQYBWMQJGPBVMNRCRENOXKGKTVIXHPLCMSTMUAHPVUYDOMPPYLEJMT↖
       PZCFBTBYMTSXKRKPGGWRLVEPODMDCHPZ", ""];
```

In[94]:=
```
MapIndexed[#2 ~Join~ {Count[#, True]} &, Table[
  SameQ[ciphertext[[i]], ciphertext[[i + j]]], {j, 30}, {i, Length[ciphertext] - j}]]
```

Out[94]=
```
{{1, 11}, {2, 15}, {3, 11}, {4, 16}, {5, 24}, {6, 12}, {7, 25}, {8, 18},
 {9, 14}, {10, 29}, {11, 11}, {12, 10}, {13, 14}, {14, 14}, {15, 34}, {16, 16},
 {17, 10}, {18, 25}, {19, 16}, {20, 28}, {21, 18}, {22, 15}, {23, 19},
 {24, 12}, {25, 22}, {26, 14}, {27, 13}, {28, 17}, {29, 17}, {30, 47}}
```

Most coincidenses occur at 5, 10, 15, 20, ...

Guess a key length of 5

Partition Ciphertext Blocks

```
block1 = Table[ciphertext[[i]], {i, 1, Length[ciphertext], 5}]
block2 = Table[ciphertext[[i]], {i, 2, Length[ciphertext], 5}]
block3 = Table[ciphertext[[i]], {i, 3, Length[ciphertext], 5}]
block4 = Table[ciphertext[[i]], {i, 4, Length[ciphertext], 5}]
block5 = Table[ciphertext[[i]], {i, 5, Length[ciphertext], 5}]
```

Out[95]= {A, W, G, N, E, Y, D, T, B, S, R, E, A, H, G, I, D, E, I, E, E, I, H, K, I, W, A, B, H, P, R, C,
R, O, I, W, S, S, B, H, T, E, O, C, S, N, A, S, W, N, R, N, W, D, L, H, L, T, T, A, R, V, L,
A, U, H, R, L, R, A, A, Y, N, D, R, E, B, G, N, N, K, H, S, H, D, Y, T, B, T, K, R, O, H}

Out[96]= {W, L, T, R, E, E, Z, E, J, T, Z, M, Y, L, Y, Y, Z, Z, N, S, P, Y, P, S, D, L, O, F, L, T, P, Z,
D, Y, E, S, E, P, Z, Z, L, H, F, E, Z, G, E, Z, L, D, T, S, Y, L, W, P, O, S, O, O, Q, P, P,
Y, A, P, E, P, P, V, O, N, H, M, E, E, W, P, R, O, T, P, T, P, O, L, P, T, S, P, L, D, P}

Out[97]= {Q, A, V, B, D, Q, N, Q, P, A, V, I, L, D, W, O, W, Z, M, I, X, B, J, M, B, A, Q, B, L, K, A, V,
I, A, I, I, P, W, W, C, T, Q, B, C, Z, M, Q, A, A, Q, V, M, U, A, I, K, N, M, I, M, M, Z, M,
L, Q, B, P, I, W, Q, I, P, W, M, P, Z, M, B, C, X, V, L, M, V, M, E, Z, B, X, G, V, M, Z}

Out[98]= {E, D, P, Q, G, T, U, P, G, V, V, P, Q, K, V, V, P, V, U, F, G, Q, Q, T, G, T, P, K, P, V, Q, X,
V, K, P, V, G, H, M, I, K, V, R, T, E, T, Q, J, E, F, I, T, K, Y, U, Q, Q, J, A, J, G, A,
R, U, F, J, G, U, H, P, K, C, W, Y, V, Q, Q, V, R, K, I, C, U, U, P, J, C, Y, K, G, E, D}

Out[99]= {I, I, M, K, V, I, M, K, V, I, L, O, J, R, L, S, G, A, L, T, H, X, S, W, V, I, K, X, S, Y, V, I,
M, R, H, M, Y, E, X, L, G, L, M, I, S, W, R, I, S, I, M, S, R, I, W, Y, V, S, Q, I, P, W,
C, X, A, I, T, Y, Q, K, W, M, P, S, L, Y, J, M, E, G, X, M, A, Y, P, M, F, M, R, W, P, C}

Count Letter Frequencies

In[119]:=
```
freq1 = Rule[First[#], N[Last[#] / Length[block1]]] & /@ Tally[block1]
freq2 = Rule[First[#], N[Last[#] / Length[block2]]] & /@ Tally[block2]
freq3 = Rule[First[#], N[Last[#] / Length[block3]]] & /@ Tally[block3]
freq4 = Rule[First[#], N[Last[#] / Length[block4]]] & /@ Tally[block4]
freq5 = Rule[First[#], N[Last[#] / Length[block5]]] & /@ Tally[block5]
```

Out[119]=
```
{A → 0.0860215, W → 0.0537634, G → 0.0322581, N → 0.0752688, E → 0.0752688,
 Y → 0.0322581, D → 0.0537634, T → 0.0645161, B → 0.0537634, S → 0.0645161,
 R → 0.0967742, H → 0.0967742, I → 0.0537634, K → 0.0322581, P → 0.0107527,
 C → 0.0215054, O → 0.0322581, L → 0.0430108, V → 0.0107527, U → 0.0107527}
```

Out[120]=
```
{W → 0.0322581, L → 0.0967742, T → 0.0752688, R → 0.0215054, E → 0.107527,
 Z → 0.0967742, J → 0.0107527, M → 0.0215054, Y → 0.0752688, N → 0.0215054,
 S → 0.0645161, P → 0.172043, D → 0.0430108, O → 0.0752688, F → 0.0215054,
 H → 0.0215054, G → 0.0107527, Q → 0.0107527, A → 0.0107527, V → 0.0107527}
```

Out[121]=
```
{Q → 0.0967742, A → 0.0860215, V → 0.0752688, B → 0.0860215,
 D → 0.0215054, N → 0.0215054, P → 0.0537634, I → 0.0967742,
 L → 0.0430108, W → 0.0645161, O → 0.0107527, Z → 0.0645161,
 M → 0.139785, X → 0.0322581, J → 0.0107527, K → 0.0215054, C → 0.0322581,
 T → 0.0107527, U → 0.0107527, E → 0.0107527, G → 0.0107527}
```

Out[122]=
```
{E → 0.0434783, D → 0.0217391, P → 0.0978261, Q → 0.108696, G → 0.0869565,
 T → 0.0652174, U → 0.076087, V → 0.119565, K → 0.0869565, F → 0.0326087,
 X → 0.0108696, H → 0.0217391, M → 0.0108696, I → 0.0326087, R → 0.0326087,
 J → 0.0543478, Y → 0.0326087, A → 0.0217391, C → 0.0326087, W → 0.0108696}
```

Out[123]=
```
{I → 0.130435, M → 0.119565, K → 0.0434783, V → 0.0543478, L → 0.0652174, O → 0.0108696,
 J → 0.0217391, R → 0.0543478, S → 0.0869565, G → 0.0326087, A → 0.0326087,
 T → 0.0217391, H → 0.0217391, X → 0.0543478, W → 0.0652174, Y → 0.0652174,
 E → 0.0217391, Q → 0.0217391, P → 0.0434783, C → 0.0217391, F → 0.0108696}
```

Convert Frequencies To Vector

In[126]:=
```
nullfreq = Rule[#, 0] & /@ CharacterRange["A", "Z"]
```

Out[126]=
```
{A → 0, B → 0, C → 0, D → 0, E → 0, F → 0, G → 0, H → 0, I → 0, J → 0, K → 0, L → 0, M → 0,
 N → 0, O → 0, P → 0, Q → 0, R → 0, S → 0, T → 0, U → 0, V → 0, W → 0, X → 0, Y → 0, Z → 0}
```

In[128]:=
```
vector1 = (CharacterRange["A", "Z"] /. freq1) /. nullfreq
vector2 = (CharacterRange["A", "Z"] /. freq2) /. nullfreq
vector3 = (CharacterRange["A", "Z"] /. freq3) /. nullfreq
vector4 = (CharacterRange["A", "Z"] /. freq4) /. nullfreq
vector5 = (CharacterRange["A", "Z"] /. freq5) /. nullfreq
```

Out[128]=
```
{0.0860215, 0.0537634, 0.0215054, 0.0537634, 0.0752688, 0, 0.0322581, 0.0967742,
 0.0537634, 0, 0.0322581, 0.0430108, 0, 0.0752688, 0.0322581, 0.0107527, 0,
 0.0967742, 0.0645161, 0.0645161, 0.0107527, 0.0107527, 0.0537634, 0, 0.0322581, 0}
```

Out[129]=
```
{0.0107527, 0, 0, 0.0430108, 0.107527, 0.0215054, 0.0107527, 0.0215054, 0, 0.0107527,
 0, 0.0967742, 0.0215054, 0.0215054, 0.0752688, 0.172043, 0.0107527, 0.0215054,
 0.0645161, 0.0752688, 0, 0.0107527, 0.0322581, 0, 0.0752688, 0.0967742}
```

Out[130]=
```
{0.0860215, 0.0860215, 0.0322581, 0.0215054, 0.0107527, 0, 0.0107527, 0, 0.0967742,
 0.0107527, 0.0215054, 0.0430108, 0.139785, 0.0215054, 0.0107527, 0.0537634,
 0.0967742, 0, 0, 0.0107527, 0.0107527, 0.0752688, 0.0645161, 0.0322581, 0, 0.0645161}
```

Out[131]=
```
{0.0217391, 0, 0.0326087, 0.0217391, 0.0434783, 0.0326087, 0.0869565, 0.0217391,
 0.0326087, 0.0543478, 0.0869565, 0, 0.0108696, 0, 0, 0.0978261, 0.108696,
 0.0326087, 0, 0.0652174, 0.076087, 0.119565, 0.0108696, 0.0108696, 0.0326087, 0}
```

Out[132]=
```
{0.0326087, 0, 0.0217391, 0, 0.0217391, 0.0108696, 0.0326087, 0.0217391, 0.130435,
 0.0217391, 0.0434783, 0.0652174, 0.119565, 0, 0.0108696, 0.0434783, 0.0217391,
 0.0543478, 0.0869565, 0.0217391, 0, 0.0543478, 0.0652174, 0.0543478, 0.0652174, 0}
```

Dot Vectors with Shifted English Frequencies

In[133]:=
```
EnglishShift[n_] :=
 RotateRight[{0.082, 0.015, 0.028, 0.043, 0.127, 0.022, 0.020, 0.061,
   0.070, 0.002, 0.008, 0.040, 0.024, 0.067, 0.075, 0.019, 0.001, 0.060,
   0.063, 0.091, 0.028, 0.010, 0.023, 0.001, 0.02, 0.001}, n]
```

In[171]:=
```
Table[{i, Dot[vector1, EnglishShift[i]]}, {i, 0, 25}]
SortBy[%, Last][[-1]]

Table[{i, Dot[vector2, EnglishShift[i]]}, {i, 0, 25}]
SortBy[%, Last][[-1]]

Table[{i, Dot[vector3, EnglishShift[i]]}, {i, 0, 25}]
SortBy[%, Last][[-1]]

Table[{i, Dot[vector4, EnglishShift[i]]}, {i, 0, 25}]
SortBy[%, Last][[-1]]

Table[{i, Dot[vector5, EnglishShift[i]]}, {i, 0, 25}]
SortBy[%, Last][[-1]]
```

Out[171]= {{0, 0.0583226}, {1, 0.0305484}, {2, 0.0302796}, {3, 0.0437957}, {4, 0.0421828},
{5, 0.0336237}, {6, 0.0353548}, {7, 0.0400968}, {8, 0.0323763}, {9, 0.0392796},
{10, 0.0392151}, {11, 0.039043}, {12, 0.031086}, {13, 0.0466129},
{14, 0.0430538}, {15, 0.0457634}, {16, 0.0348602}, {17, 0.0335376},
{18, 0.0366129}, {19, 0.0410323}, {20, 0.0370753}, {21, 0.0307097},
{22, 0.0453226}, {23, 0.0333333}, {24, 0.0340215}, {25, 0.0438602}}

Out[172]= {0, 0.0583226}

Out[173]= {{0, 0.0478172}, {1, 0.0415591}, {2, 0.0313548}, {3, 0.0335161},
{4, 0.0395484}, {5, 0.0336667}, {6, 0.0349892}, {7, 0.0510215}, {8, 0.0367097},
{9, 0.023043}, {10, 0.0386344}, {11, 0.0716129}, {12, 0.0406237},
{13, 0.0323333}, {14, 0.0329785}, {15, 0.041086}, {16, 0.0294731}, {17, 0.036},
{18, 0.0385054}, {19, 0.0334839}, {20, 0.0312581}, {21, 0.0388602},
{22, 0.0477742}, {23, 0.0409247}, {24, 0.0383118}, {25, 0.035914}}

Out[174]= {11, 0.0716129}

Out[175]= {{0, 0.0307742}, {1, 0.0351075}, {2, 0.034086}, {3, 0.0332043}, {4, 0.0462581},
{5, 0.0334839}, {6, 0.0285484}, {7, 0.0392796}, {8, 0.0689247}, {9, 0.041828},
{10, 0.0315161}, {11, 0.0316452}, {12, 0.0474731}, {13, 0.0323763},
{14, 0.0341183}, {15, 0.0366989}, {16, 0.0335806}, {17, 0.0332151},
{18, 0.0372903}, {19, 0.0445806}, {20, 0.0401398}, {21, 0.0449355},
{22, 0.0396452}, {23, 0.0470323}, {24, 0.0391935}, {25, 0.0360645}}

Out[176]= {8, 0.0689247}

Out[177]= {{0, 0.0303804}, {1, 0.040087}, {2, 0.0637935}, {3, 0.0428913}, {4, 0.0362174},
{5, 0.0328696}, {6, 0.0416848}, {7, 0.0364891}, {8, 0.0397391}, {9, 0.0323152},
{10, 0.0310326}, {11, 0.0353696}, {12, 0.044337}, {13, 0.0442391},
{14, 0.0337174}, {15, 0.0419022}, {16, 0.0451304}, {17, 0.0497717},
{18, 0.0347174}, {19, 0.033837}, {20, 0.0287283}, {21, 0.0345326},
{22, 0.0363152}, {23, 0.038337}, {24, 0.040663}, {25, 0.0319022}}

Out[178]= {2, 0.0637935}

Out[179]= {{0, 0.0390435}, {1, 0.0332283}, {2, 0.0322391}, {3, 0.0358261}, {4, 0.0623043},
{5, 0.0436087}, {6, 0.034}, {7, 0.0380543}, {8, 0.0497717}, {9, 0.0319783},
{10, 0.0379022}, {11, 0.0358804}, {12, 0.0332826}, {13, 0.0299783},
{14, 0.0389674}, {15, 0.0419674}, {16, 0.0353804}, {17, 0.0406957},
{18, 0.0413804}, {19, 0.0438261}, {20, 0.0430217}, {21, 0.0363913},
{22, 0.0323152}, {23, 0.0348696}, {24, 0.0417391}, {25, 0.0333478}}

Out[180]= {4, 0.0623043}

Max Dot Products Occur At:

In[191]:=
```
FromCharacterCode[0 + 65]
FromCharacterCode[11 + 65]
FromCharacterCode[8 + 65]
FromCharacterCode[2 + 65]
FromCharacterCode[4 + 65]
```

Out[191]= A

Out[192]= L

Out[193]= I

Out[194]= C

Out[195]= E

The key is: "**alice**"

Decrypt Message

In[196]:=
```
ciphertext
```

Out[196]=
```
{A, W, Q, E, I, W, L, A, D, I, G, T, V, P, M, N, R, B, Q, K, E, E, D, G, V, Y, E, Q, T, I,
 D, Z, N, U, M, T, E, Q, P, K, B, J, P, G, V, S, T, A, V, I, R, Z, V, V, L, E, M, I, P,
 O, A, Y, L, Q, J, H, L, D, K, R, G, Y, W, V, L, I, Y, O, V, S, D, Z, W, P, G, E, Z, Z,
 V, A, I, N, M, U, L, E, S, I, F, T, E, P, X, G, H, I, Y, B, Q, X, H, P, J, Q, S, K, S,
 M, T, W, I, D, B, G, V, W, L, A, T, I, A, O, Q, P, K, B, F, B, K, X, H, L, L, P, S, P,
 T, K, V, Y, R, P, A, Q, V, C, Z, V, X, I, R, D, I, V, M, O, Y, A, K, R, I, E, I, P, H,
 W, S, I, V, M, S, E, P, G, Y, S, P, W, H, E, B, Z, W, M, X, H, Z, C, I, L, T, L, T, K,
 G, E, H, Q, V, L, O, F, B, R, M, C, E, C, T, I, S, Z, Z, E, S, N, G, M, T, W, A, E, Q,
 Q, R, S, Z, A, J, I, W, L, A, E, S, N, D, Q, F, I, R, T, V, I, M, N, S, M, T, S, W, Y,
 U, K, R, D, L, A, Y, I, L, W, I, U, W, H, P, K, Q, Y, L, O, N, Q, V, T, S, M, J, S, T,
 O, I, A, Q, A, O, M, J, I, R, Q, M, G, P, V, P, Z, A, W, L, P, M, R, C, A, Y, L, U, X,
 U, A, Q, F, A, H, P, B, J, I, R, E, P, G, T, L, P, I, U, Y, R, P, W, H, Q, A, V, Q, P,
 K, A, O, I, K, W, Y, N, P, C, M, N, H, W, W, P, D, M, M, Y, S, R, E, P, V, L, E, E, Z,
 Q, Y, B, W, M, Q, J, G, P, B, V, M, N, R, C, R, E, N, O, X, K, G, K, T, V, I, X, H, P,
 L, C, M, S, T, M, U, A, H, P, V, U, Y, D, O, M, P, P, Y, L, E, J, M, T, P, Z, C, F,
 B, T, B, Y, M, T, S, X, K, R, K, P, G, G, W, R, L, V, E, P, O, D, M, D, C, H, P, Z}
```

In[199]:=
```
key = PadRight[{}, Length[ciphertext], {"A", "L", "I", "C", "E"}]
```

Out[199]=
```
{A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E,
 A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C,
 E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I,
 C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L,
 I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A,
 L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E,
 A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C,
 E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I,
 C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L,
 I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A,
 L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E,
 A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C,
 E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I,
 C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L,
 I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E,
 A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I, C, E, A, L, I}
```

Subtract key from ciphertext

In[215]:=
```
FromCharacterCode[
 Mod[Flatten[ToCharacterCode /@ ciphertext - ToCharacterCode /@ key] + 97, 26, 97]]
```

Out[215]=
```
alicewasbeginningtogetverytiredofsittingbyhersisteronthebankandofhavingnothingtod
   oonceortwiceshehadpeepedintothebookhersisterwasreadingbutithadnopicturesorcon
   versationsinitandwhatistheuseofabookthoughtalicewithoutpicturesorconversation
   soshewasconsideringinherownmindaswellasshecouldforthehotdaymadeherfeelverysle
   epyandstupidwhetherthepleasureofmakingadaisychainwouldbeworththetroubleofgett
   ingupandpickingthedaisieswhensuddenlyawhiterabbitwithpinkeyesranclosebyher
```

Question 2

Build Polybius Square

```
StringSplit["PERSPECTIVE", ""]
key = DeleteDuplicates[%]
```

Out[219]=
```
{P, E, R, S, P, E, C, T, I, V, E}
```

Out[220]=
```
{P, E, R, S, C, T, I, V}
```

```
CharacterRange["A", "Z"]
Select[%, ! MemberQ[key, #] &]
remainingLetters = DeleteCases[remainingLetters, "J"]
```

Out[233]=
```
{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z}
```

Out[234]=
```
{A, B, D, F, G, H, J, K, L, M, N, O, Q, U, W, X, Y, Z}
```

Out[235]=
```
{A, B, D, F, G, H, K, L, M, N, O, Q, U, W, X, Y, Z}
```

In[236]:=
```
polybius = Partition[Join[key, remainingLetters], 5];
TableForm[%]
```

Out[237]//TableForm=

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

Pad and Block Plaintext

In[292]:=
```
plaintext = StringSplit[ToUpperCase[StringReplace[
     "whenyouhaveahammereverythingjustlookslikeanail", {"j" → "i"}]], ""]

blocktext = {};
While[plaintext ≠ {},
  If[
    Length[plaintext] == 1,
    AppendTo[blocktext, {First[plaintext], "X"}];
    plaintext = {};,  (* Last letter; pad with "X" *)

    If[
     plaintext[[1]] == plaintext[[2]],  (* Same letter in block; pad with "X" *)
     AppendTo[blocktext, {First[plaintext], "X"}]; plaintext = Drop[plaintext, 1];,

     (* Different letters *)
     AppendTo[blocktext, plaintext[[1 ;; 2]]]; plaintext = Drop[plaintext, 2];
    ]
   ];
 ];
blocktext
```

Out[292]=
```
{W, H, E, N, Y, O, U, H, A, V, E, A, H, A, M, M, E, R, E, V, E, R,
 Y, T, H, I, N, G, I, U, S, T, L, O, O, K, S, L, I, K, E, A, N, A, I, L}
```

Out[295]=
```
{{W, H}, {E, N}, {Y, O}, {U, H}, {A, V}, {E, A}, {H, A},
 {M, X}, {M, E}, {R, E}, {V, E}, {R, Y}, {T, H}, {I, N}, {G, I},
 {U, S}, {T, L}, {O, X}, {O, K}, {S, L}, {I, K}, {E, A}, {N, A}, {I, L}}
```

Implement Encryption Cipher

In[272]:=
```
EncryptPlayfair[square_, {letter1_, letter2_}] :=
 Module[
  {
   pos1 = Position[square, letter1][[1]],
   pos2 = Position[square, letter2][[1]],
   newLetter1,
   newLetter2
  },

  Which[
   First[pos1] == First[pos2],  (* Check if letters are on the same row *)
   newLetter1 = Extract[square, {pos1[[1]], Mod[pos1[[2]] + 1, 5, 1]}];
   newLetter2 = Extract[square, {pos2[[1]], Mod[pos2[[2]] + 1, 5, 1]}];
   ,
   Last[pos1] == Last[pos2],  (* Check if letters are on the same column *)
   newLetter1 = Extract[square, {Mod[pos1[[1]] + 1, 5, 1], pos1[[2]]}];
   newLetter2 = Extract[square, {Mod[pos2[[1]] + 1, 5, 1], pos2[[2]]}];
   ,
   True,  (* Letter are on different rows and columns *)
   newLetter1 = Extract[square, {pos1[[1]], pos2[[2]]} ];
   newLetter2 = Extract[square, {pos2[[1]], pos1[[2]]}];
  ];

  Return[{newLetter1, newLetter2}];
 ]
```

Encrypt

In[301]:=
```
EncryptPlayfair[polybius, #] & /@ blocktext
StringJoin[Flatten[%]]
```

Out[301]=
```
{{Y, F}, {R, M}, {S, Y}, {Y, D}, {B, A}, {S, I}, {O, H},
 {N, W}, {W, I}, {S, R}, {I, R}, {S, X}, {A, D}, {V, M}, {F, V},
 {Y, P}, {D, U}, {N, Y}, {Q, H}, {P, O}, {B, F}, {S, I}, {O, V}, {T, M}}
```

Out[302]=
```
YFRMSYYDBASIOHNWWISRIRSXADVMFVYPDUNYQHPOBFSIOVTM
```

Question 3

Re-block the ciphertext

Since the key: **SMILE** is 5 letters long, and the cipher text is

In[322]:=
```
key = "SMILE";
StringLength[key]

ciphertext = StringSplit[
   "XDDXDXXAFXFGDXGAGXXDGGXADFFGXGDDXAGDGDDXDAXGDFXDFFDFXDXFDDXGGAXFGAXFFADFDDAX
      DGFXFFFGAGDDAAFXGGGADXGDGFFXGFGDDGFFFDGDGGGXGDGG", ""];
Length[ciphertext]
```

Out[323]= 5

Out[325]= 124

In[326]:=
```
Quotient[124, 5]
Mod[124, 5]
```

Out[326]= 24

Out[327]= 4

The last row will only have **4** letters among the 5 columns

From the alphabetical order of the key (S,M,I,L,E) → (E, I, L, M, S) the “E” (1st) column should have one less letter

In[341]:=
```
{
 Append[ciphertext[[1 ;; 24]], " "],
 ciphertext[[25 ;; 49]],
 ciphertext[[50 ;; 74]],
 ciphertext[[75 ;; 99]],
 ciphertext[[100 ;; 124]]
}

block = Transpose[%];
TableForm[block]
```

Out[341]=
```
{{X, D, D, X, D, X, X, A, F, X, F, G, D, X, G, A, G, X, X, D, G, G, X, A,  },
 {D, F, F, G, X, G, D, D, X, A, G, D, G, D, D, X, D, A, X, G, D, F, X, D, F},
 {F, D, F, X, D, X, F, D, D, X, G, G, A, X, F, G, A, X, F, F, A, D, F, D, D},
 {A, X, D, G, F, X, F, F, F, G, A, G, D, D, A, A, F, X, G, G, G, A, D, X, G},
 {D, G, F, F, X, G, F, G, D, D, G, F, F, F, D, G, D, G, G, G, X, G, D, G, G}}
```

Out[343]//TableForm=

X	D	F	A	D
D	F	D	X	G
D	F	F	D	F
X	G	X	G	F
D	X	D	F	X
X	G	X	X	G
X	D	F	F	F
A	D	D	F	G
F	X	D	F	D
X	A	X	G	D
F	G	G	A	G
G	D	G	G	F
D	G	A	D	F
X	D	X	D	F
G	D	F	A	D
A	X	G	A	G
G	D	A	F	D
X	A	X	X	G
X	X	F	G	G
D	G	F	G	G
G	D	A	G	X
G	F	D	A	G
X	X	F	D	D
A	D	D	X	G
	F	D	G	G

Un-alphabetize the key

(E, I, L, M, S) → (S,M,I,L,E)
(1, 2, 3, 4, 5) → (5, 4, 2, 3, 1)

In[348]:=
```
newBlock = block[[All, {5, 4, 2, 3, 1}]];
TableForm[newBlock]
```

Out[349]//TableForm=

D	A	D	F	X
G	X	F	D	D
F	D	F	F	D
F	G	G	X	X
X	F	X	D	D
G	X	G	X	X
F	F	D	F	X
G	F	D	D	A
D	F	X	D	F
D	G	A	X	X
G	A	G	G	F
F	G	D	G	G
F	D	G	A	D
F	D	D	X	X
D	A	D	F	G
G	A	X	G	A
D	F	D	A	G
G	X	A	X	X
G	G	X	F	X
G	G	G	F	D
X	G	D	A	G
G	A	F	D	G
D	D	X	F	X
G	X	D	D	A
G	G	F	D	

Divide Row-by-Row into Blocks of 2

In[354]:=
```
codeblock = Partition[Most[Flatten[newBlock]], 2]
```

Out[354]=
```
{{D, A}, {D, F}, {X, G}, {X, F}, {D, D}, {F, D}, {F, F}, {D, F}, {G, G}, {X, X}, {X, F},
 {X, D}, {D, G}, {X, G}, {X, X}, {F, F}, {D, F}, {X, G}, {F, D}, {D, A}, {D, F}, {X, D},
 {F, D}, {G, A}, {X, X}, {G, A}, {G, G}, {F, F}, {G, D}, {G, G}, {F, D}, {G, A},
 {D, F}, {D, D}, {X, X}, {D, A}, {D, F}, {G, G}, {A, X}, {G, A}, {D, F}, {D, A},
 {G, G}, {X, A}, {X, X}, {G, G}, {X, F}, {X, G}, {G, G}, {F, D}, {X, G}, {D, A},
 {G, G}, {A, F}, {D, G}, {D, D}, {X, F}, {X, G}, {X, D}, {D, A}, {G, G}, {F, D}}
```

Decode Using the Polybius Square

In[353]:=
```
polySquare = {{"A", "A"} → "k", {"A", "D"} → "p",
    {"A", "F"} → "b", {"A", "G"} → "z", {"A", "X"} → "u", {"D", "A"} → "t",
    {"D", "D"} → "a", {"D", "F"} → "h", {"D", "G"} → "l", {"D", "X"} → "v",
    {"F", "A"} → "d", {"F", "D"} → "n", {"F", "F"} → "w", {"F", "G"} → "y",
    {"F", "X"} → "q", {"G", "A"} → "g", {"G", "D"} → "r", {"G", "F"} → "x",
    {"G", "G"} → "o", {"G", "X"} → "c", {"X", "A"} → "f", {"X", "D"} → "i",
    {"X", "F"} → "m", {"X", "G"} → "e", {"X", "X"} → "s"};
```

In[355]:=
```
codeblock /. polySquare
```

Out[355]=
```
{t, h, e, m, a, n, w, h, o, s, m, i, l, e, s, w, h, e, n, t, h, i, n, g, s, g, o, w, r, o, n, g,
 h, a, s, t, h, o, u, g, h, t, o, f, s, o, m, e, o, n, e, t, o, b, l, a, m, e, i, t, o, n}
```

Question 4

Mathematica has built-in fuctions to compute these values directly:

In[395]:=
```
M = {{15, 5, 18}, {13, 22, 24}, {17, 19, 7}};
Det[M]
Inverse[M, Modulus → 26] // MatrixForm
```

Out[396]= -5231

Out[397]//MatrixForm=

$$\begin{pmatrix} 24 & 1 & 24 \\ 25 & 9 & 20 \\ 15 & 14 & 25 \end{pmatrix}$$

To recieve credit, must show work:

Compute det(M):

$$\begin{vmatrix} 15 & 5 & 18 \\ 13 & 22 & 24 \\ 17 & 19 & 7 \end{vmatrix} = 15 \begin{vmatrix} 22 & 24 \\ 19 & 7 \end{vmatrix} - 13 \begin{vmatrix} 5 & 18 \\ 19 & 7 \end{vmatrix} + 17 \begin{vmatrix} 5 & 18 \\ 22 & 24 \end{vmatrix}$$

$$= 15\,(22\times 7 - 24\times 19) - 13\,(5\times 7 - 18\times 19) + 17\,(5\times 24 - 22\times 18)$$
$$= -5,\,231$$

Compute M^{-1}(mod 26):

$$\left(\begin{array}{cccccc} 15 & 5 & 18 & 1 & 0 & 0 \\ 13 & 22 & 24 & 0 & 1 & 0 \\ 17 & 19 & 7 & 0 & 0 & 1 \end{array}\right) \pmod{26} \qquad 15^{-1} \equiv 7 \pmod{26}$$

$r_1 \to 7\,r_1$
$$\left(\begin{array}{cccccc} 1 & 9 & 22 & 7 & 0 & 0 \\ 13 & 22 & 24 & 0 & 1 & 0 \\ 17 & 19 & 7 & 0 & 0 & 1 \end{array}\right) \pmod{26}$$

$r_2 \to r_2 - 13\,r_1$
$$\left(\begin{array}{cccccc} 1 & 9 & 22 & 7 & 0 & 0 \\ 0 & 9 & 24 & 13 & 1 & 0 \\ 17 & 19 & 7 & 0 & 0 & 1 \end{array}\right) \pmod{26}$$

$r_3 \to r_3 - 17\,r_1$
$$\left(\begin{array}{cccccc} 1 & 9 & 22 & 7 & 0 & 0 \\ 0 & 9 & 24 & 13 & 1 & 0 \\ 0 & 22 & 23 & 11 & 0 & 1 \end{array}\right) \pmod{26} \qquad 9^{-1} \equiv 3 \pmod{26}$$

$r_2 \to 3\,r_2$
$$\left(\begin{array}{cccccc} 1 & 9 & 22 & 7 & 0 & 0 \\ 0 & 1 & 20 & 13 & 3 & 0 \\ 0 & 22 & 23 & 11 & 0 & 1 \end{array}\right) \pmod{26}$$

$$r_3 \to r_3 - 22\, r_2 \qquad \begin{pmatrix} 1 & 9 & 22 & 7 & 0 & 0 \\ 0 & 1 & 20 & 13 & 3 & 0 \\ 0 & 0 & 25 & 11 & 12 & 1 \end{pmatrix} \pmod{26} \qquad 25^{-1} \equiv 25 \pmod{26}$$

$$r_3 \to 25\, r_3 \qquad \begin{pmatrix} 1 & 9 & 22 & 7 & 0 & 0 \\ 0 & 1 & 20 & 13 & 3 & 0 \\ 0 & 0 & 1 & 15 & 14 & 25 \end{pmatrix} \pmod{26}$$

$$r_2 \to r_2 - 20\, r_3 \qquad \begin{pmatrix} 1 & 9 & 22 & 7 & 0 & 0 \\ 0 & 1 & 0 & 25 & 9 & 20 \\ 0 & 0 & 1 & 15 & 14 & 25 \end{pmatrix} \pmod{26}$$

$$r_1 \to r_1 - 22\, r_3 \qquad \begin{pmatrix} 1 & 9 & 0 & 15 & 4 & 22 \\ 0 & 1 & 0 & 25 & 9 & 20 \\ 0 & 0 & 1 & 15 & 14 & 25 \end{pmatrix} \pmod{26}$$

$$r_1 \to r_1 - 9\, r_2 \qquad \begin{pmatrix} 1 & 0 & 0 & 24 & 1 & 24 \\ 0 & 1 & 0 & 25 & 9 & 20 \\ 0 & 0 & 1 & 15 & 14 & 25 \end{pmatrix} \pmod{26}$$

Question 5

In[388]:=
```
B = {{1, 24, 1}, {0, 8, 3}, {21, 9, 26}};
MatrixForm[B]
```

Out[389]//MatrixForm=

$$\begin{pmatrix} 1 & 24 & 1 \\ 0 & 8 & 3 \\ 21 & 9 & 26 \end{pmatrix}$$

In[390]:=
```
codeBlocks = Partition[ToCharacterCode["thecakeisaliexx"], 3] - 97
```

Out[390]= {{19, 7, 4}, {2, 0, 10}, {4, 8, 18}, {0, 11, 8}, {4, 23, 23}}

In[391]:=
```
Mod[Dot[#, M], 26] & /@ codeBlocks
FromCharacterCode /@ (% + 97)
ToUpperCase[StringJoin[%]]
```

Out[391]= {{25, 2, 14}, {4, 8, 2}, {18, 10, 2}, {12, 4, 7}, {19, 19, 21}}

Out[392]= {zco, eic, skc, meh, ttv}

Out[393]= ZCOEICSKCMEHTTV

In[421]:=
```
Inverse[B, Modulus → 26] // MatrixForm
```

Out[421]//MatrixForm=

$$\begin{pmatrix} 3 & 25 & 16 \\ 19 & 11 & 9 \\ 10 & 23 & 2 \end{pmatrix}$$