Lecture Notes

Advanced Discrete Structures
COT 4115.001 S15

2015-01-20

Recall

- **Shift ciphers**
- **Affine ciphers**
- **Vigenere ciphers**

- **Chapter 2 - Classical Cryptosystems**

Section 2.3 - Vigenère Cipher

Vigenère Cipher - Example

```
ciphertext =
  "ZWQOKKUTHVVGEVSHVPELRTFIPPDGIHWBJAEVWAORRLNQDSNLPPTNTOAPDNIBSPNWRVWNZRDHNIMDRXJBDMN
     KKEZSKKANZRDHNAVIWHPPDIIKKCRENDOALACOBWQTYHHCLBVUPWAUZOZQSHRGPWAETDNZHEUEUEZGF
     QIIMYDLHMRTYHNMVEIHBWTRNDHTRAWOKWQAEGWZNOWZDQBHDDZMNNVUKWLAEGPPHSIRKUBOEWWQMEU
     DNCRTPOKWJIEJYWNKJWKDDATXLJNAIGBWQTYHZQRHVVWBZBCHPPQEVRNNNUIFDIHRJDJLSHVEALRUE
     FHMGEEUUIMDRXJBDMYDZIAIXEALHNFQAKNREHNIMDURNWSHPDHQSTCHXMCIEDJWSHVUYWQNVUPPDRV
     ZWAMOXDNZDTRWWTKAEGJWBECOWZDXTHLBZSDDHTGOCHZCFIEWDMFRFXJLBACOALZCPFHWMETHHTZRN
     KAZDTYHBILICBYWTLUJKQMCRVAWMEFIPPNSVJNMZTNKEZKWZQZAZRFVAUHGYWUMMOLJDBNCIXOPZNP
     EQQKDZQCQMIKVLISHZWSIRRVDYPDDSBWBQAGGKWQIEWDMLIUGHMNFKKANKOFUBZNMNKEKGACDZLDRC
     HZLNWELJBNTYHOUZLCGWZJHFOAEGEEGKZNTYBOBNOULJBGEURKZVAPDJLKOFNALZRFXJLRHVFKCKDJ
     HAVNTYLJOAUKWDMFRVDPOQAPSNIHRZHKVDVVUUAHDVQKBZTIHAVNRRKKCRESUKSDTYHXZNAUVSMDPF
     IBTZTTRQVSRPWDISRVDYPDDKRPPDEUJAWETYHOSXIEDHTCIIHYBHOEVPPDSLQDICBRNALSHVSHWVEU
     OWVCIEWKIFRRBIIRSNLPPKIKWHMBRRFGAQUEQEVFTYUKCFHZWADDNKKAOQAJVSIRNFWCZDEEIKZSHV
     VQVGAUEQZMEUWDMSOGVKNSHVOKVFBCDZMRUEWETSHVBSMQEKKAAZMVJNIXCFOKZSOSHOMDNVYAZXWY
     HNMNNTHPPDHFXOMGAUEAMMPRLJBDDSXPBGEJXJJKIJWAZDDKKAXZIEWWVCTYHNIHNJZWAGEULPIVAP
     DJLMONWDMGOLVAEZSRVZCKLRQZOQAPDOMUEIBPPHNXHHAD";
```

Vigenère Cipher - Guessing Key Length

Shifts and Coincidences

For each $k \in \mathbb{Z}$, **shift** the ciphertext k places to the right an count the **coincidences**, i.e., places where the ciphertext and shifted-ciphertext agree.

```
k = 3;
TableForm[Transpose[Table[StringTake[ciphertext, {{i}, {i + k}}], {i, 15}]]]
Table[MatchQ @@ StringTake[ciphertext, {{i}, {i + k}}], {i, 15}]
Count[%, True]
```

```
Z    W    Q    O    K    K    U    T    H    V    V    G    E    V    S
O    K    K    U    T    H    V    V    G    E    V    S    H    V    P
```

```
{False, False, False, False, False, False,
 False, False, False, False, True, False, False, True, False}
```

```
2
```

Guess Key Length

Most frequent is best guess for key length:

```
MapIndexed[{#2[[1]], Count[#, True]} &,
 Table[MatchQ @@ StringTake[ciphertext, {{i}, {i + k}}],
  {k, 15}, {i, StringLength[ciphertext] - k}]]
```

```
{{1, 64}, {2, 30}, {3, 43}, {4, 41}, {5, 59}, {6, 70}, {7, 36},
 {8, 39}, {9, 44}, {10, 33}, {11, 39}, {12, 61}, {13, 31}, {14, 47}, {15, 51}}
```

Vigenère Cipher - Frequency Anaysis

Divide into Blocks

Most frequent is best guess for key length:

```
cipherBlocks = Partition[StringSplit[ciphertext, ""], 6];
```

Frequency Analysis

Consider letter frequency of each block:

```
block1 = cipherBlocks[[All, 1]]
Sort[Tally[block1], #1[[2]] > #2[[2]] &]
{#[[1]], N[#[[2]] / Length[block1]]} & /@ %
```

```
{Z, U, E, E, P, W, W, N, P, A, S, W, N, J, K, A, N, P, K, O, B, H, P, Z, P, N, U, I, H, N, B, H, K,
 W, D, Z, K, P, K, W, N, K, Y, K, L, B, Z, W, P, N, D, J, A, H, U, J, Z, A, A, N, N, H, X, J, Y,
 P, W, N, W, J, W, L, H, Z, D, J, A, H, H, A, B, Y, K, A, P, N, E, Z, A, U, D, O, Q, C, L, S, Y,
 W, K, D, H, A, B, E, Z, Z, J, O, W, A, K, O, J, K, J, A, J, K, A, J, D, P, N, K, U, K, A, K,
 K, X, S, B, Q, D, Y, P, A, O, H, Y, P, D, A, H, W, K, I, P, H, G, E, K, A, A, S, C, K, Q, Q,
 D, K, K, Z, E, S, A, N, K, O, A, N, P, O, A, J, P, J, A, A, W, N, W, P, J, D, A, Z, Z, O, P}
```

```
{{A, 24}, {K, 22}, {P, 17}, {N, 15}, {J, 14}, {W, 14}, {H, 12}, {Z, 12}, {D, 10}, {O, 8},
 {Y, 6}, {B, 6}, {E, 6}, {S, 5}, {U, 5}, {Q, 4}, {L, 3}, {C, 2}, {X, 2}, {I, 2}, {G, 1}}
```

```
{{A, 0.126316}, {K, 0.115789}, {P, 0.0894737}, {N, 0.0789474},
 {J, 0.0736842}, {W, 0.0736842}, {H, 0.0631579}, {Z, 0.0631579},
 {D, 0.0526316}, {O, 0.0421053}, {Y, 0.0315789}, {B, 0.0315789},
 {E, 0.0315789}, {S, 0.0263158}, {U, 0.0263158}, {Q, 0.0210526}, {L, 0.0157895},
 {C, 0.0105263}, {X, 0.0105263}, {I, 0.0105263}, {G, 0.00526316}}
```

Vigenère Cipher - Block 1

English Language Frequencies

```
{{E, 0.127}, {T, 0.091}, {A, 0.082}, {O, 0.075}, {I, 0.07}, {N, 0.067},
 {S, 0.063}, {H, 0.061}, {R, 0.06}, {D, 0.043}, {L, 0.04}, {U, 0.028}, {C, 0.028},
 {M, 0.024}, {W, 0.023}, {F, 0.022}, {Y, 0.02}, {G, 0.02}, {P, 0.019}, {B, 0.015},
 {V, 0.01}, {K, 0.008}, {J, 0.002}, {Z, 0.001}, {X, 0.001}, {Q, 0.001}}
```

Block 1 Frequencies

```
{{A, 0.126316}, {K, 0.115789}, {P, 0.0894737}, {N, 0.0789474},
 {J, 0.0736842}, {W, 0.0736842}, {H, 0.0631579}, {Z, 0.0631579},
 {D, 0.0526316}, {O, 0.0421053}, {Y, 0.0315789}, {B, 0.0315789},
 {E, 0.0315789}, {S, 0.0263158}, {U, 0.0263158}, {Q, 0.0210526}, {L, 0.0157895},
 {C, 0.0105263}, {X, 0.0105263}, {I, 0.0105263}, {G, 0.00526316}}
```

Guessed Frequencies: E → A

Shift cipher with $\kappa = 0 - 4 = -4$

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

Vigenère Cipher - Block 1

English Language Frequencies

```
{{E, 0.127}, {T, 0.091}, {A, 0.082}, {O, 0.075}, {I, 0.07}, {N, 0.067},
 {S, 0.063}, {H, 0.061}, {R, 0.06}, {D, 0.043}, {L, 0.04}, {U, 0.028}, {C, 0.028},
 {M, 0.024}, {W, 0.023}, {F, 0.022}, {Y, 0.02}, {G, 0.02}, {P, 0.019}, {B, 0.015},
 {V, 0.01}, {K, 0.008}, {J, 0.002}, {Z, 0.001}, {X, 0.001}, {Q, 0.001}}
```

Block 1 Frequencies

```
{{A, 0.126316}, {K, 0.115789}, {P, 0.0894737}, {N, 0.0789474},
 {J, 0.0736842}, {W, 0.0736842}, {H, 0.0631579}, {Z, 0.0631579},
 {D, 0.0526316}, {O, 0.0421053}, {Y, 0.0315789}, {B, 0.0315789},
 {E, 0.0315789}, {S, 0.0263158}, {U, 0.0263158}, {Q, 0.0210526}, {L, 0.0157895},
 {C, 0.0105263}, {X, 0.0105263}, {I, 0.0105263}, {G, 0.00526316}}
```

Guessed Frequencies: E → K

Shift cipher with $\kappa = 10 - 4 = 6$

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

Vigenère Cipher - Block 2

- **English Language Frequencies**

```
{{E, 0.127}, {T, 0.091}, {A, 0.082}, {O, 0.075}, {I, 0.07}, {N, 0.067},
 {S, 0.063}, {H, 0.061}, {R, 0.06}, {D, 0.043}, {L, 0.04}, {U, 0.028}, {C, 0.028},
 {M, 0.024}, {W, 0.023}, {F, 0.022}, {Y, 0.02}, {G, 0.02}, {P, 0.019}, {B, 0.015},
 {V, 0.01}, {K, 0.008}, {J, 0.002}, {Z, 0.001}, {X, 0.001}, {Q, 0.001}}
```

- **Block 2 Frequencies**

```
{{M, 0.115789}, {W, 0.105263}, {I, 0.0947368}, {Z, 0.0894737},
 {P, 0.0894737}, {B, 0.0736842}, {L, 0.0684211}, {V, 0.0526316},
 {Q, 0.0473684}, {A, 0.0473684}, {C, 0.0421053}, {T, 0.0421053},
 {N, 0.0263158}, {O, 0.0210526}, {E, 0.0210526}, {U, 0.0157895}, {S, 0.0105263},
 {K, 0.0105263}, {J, 0.0105263}, {D, 0.0105263}, {X, 0.00526316}}
```

- **Guessed Frequencies: E → M**

Shift cipher with $\kappa = 12 - 4 = 8$

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

- **Shift Ciphers with κ :**

1. E → A,	2. E → M,	3. E → D,	4. E → E,	5. E → V,	6. E → H
$(\kappa = 22)$	$(\kappa = 8)$	$(\kappa = -1)$	$(\kappa = 0)$	$(\kappa = 17)$	$(\kappa = 3)$
W	I	Z	A	R	D

- **Subtract Key to Decrypt**

```
StringTake[ciphertext, 30]
Mod[ToCharacterCode[ciphertext][[1 ;; 60]] - 97, 26]
Mod[
 ToCharacterCode["WIZARDWIZARDWIZARDWIZARDWIZARDWIZARDWIZARDWIZARDWIZARDWIZARD"] - 97,
 26]
Mod[ToCharacterCode[ciphertext][[1 ;; 60]] -
  ToCharacterCode["WIZARDWIZARDWIZARDWIZARDWIZARDWIZARDWIZARDWIZARDWIZARDWIZARD"], 26]
FromCharacterCode[% + 97]
```

```
ZWQOKKUTHVVGEVSHVPELRTFIPPDGIH
```

```
{19, 16, 10, 8, 4, 4, 14, 13, 1, 15, 15, 0, 24, 15, 12, 1, 15, 9,
 24, 5, 11, 13, 25, 2, 9, 9, 23, 0, 2, 1, 16, 21, 3, 20, 24, 15, 16, 20, 8,
 11, 11, 5, 7, 10, 23, 12, 7, 5, 9, 9, 13, 7, 13, 8, 20, 9, 23, 7, 2, 21}
```

```
{16, 2, 19, 20, 11, 23, 16, 2, 19, 20, 11, 23, 16, 2, 19, 20, 11, 23, 16,
 2, 19, 20, 11, 23, 16, 2, 19, 20, 11, 23, 16, 2, 19, 20, 11, 23, 16, 2, 19, 20,
 11, 23, 16, 2, 19, 20, 11, 23, 16, 2, 19, 20, 11, 23, 16, 2, 19, 20, 11, 23}
```

```
{3, 14, 17, 14, 19, 7, 24, 11, 8, 21, 4, 3, 8, 13, 19, 7, 4, 12,
 8, 3, 18, 19, 14, 5, 19, 7, 4, 6, 17, 4, 0, 19, 10, 0, 13, 18, 0, 18, 15,
 17, 0, 8, 17, 8, 4, 18, 22, 8, 19, 7, 20, 13, 2, 11, 4, 7, 4, 13, 17, 24}
```

```
dorothylivedinthemidstofthegreatkansasprairieswithunclehenry
```

Vigenère Cipher - Find Key (Method #2)

Let $\boldsymbol{A_0}$ be a vector containing the english language frequencies:

$$A_0 = \{0.082, 0.015, 0.028, \; ... , 0.023, 0.001, 0.020, 0.001\}$$

Let $\boldsymbol{A_i}$ be a vector containing the english language frequencies shifted $\boldsymbol{i}$ places to the right. For example,

$$A_3 = \{0.001, 0.020, 0.001, 0.082, 0.015, 0.028, \; ... , 0.023\}$$

<u>Recall</u>: The **dot product** of vectors $V = \{v_1, v_2, \ldots, v_k\}$ and $W = \{w_1, w_2, \ldots, w_k\}$ is

$$V \cdot W = v_1\, w_1 + v_2\, w_2 + \ldots + v_k\, w_k$$

Thus $A_0 \cdot A_0 = (0.082)^2 + (0.015)^2 + \ldots + (0.001)^2 = 0.66$. In fact,

$$A_0 \cdot A_0 = A_1 \cdot A_1 = \ldots = A_k \cdot A_k = 0.066$$

Similarly, $A_0 \cdot A_1 = A_1 \cdot A_2 = \ldots = A_{k-1} \cdot A_k = A_k \cdot A_0 = 0.039$

Let the vector $\boldsymbol{W_i}$ be the frequencies of the letters belonging to the i^{th} block of Method #1.

- **Example**

```
{{A, 0.126316}, {K, 0.115789}, {P, 0.0894737}, {N, 0.0789474},
 {J, 0.0736842}, {W, 0.0736842}, {H, 0.0631579}, {Z, 0.0631579},
 {D, 0.0526316}, {O, 0.0421053}, {Y, 0.0315789}, {B, 0.0315789},
 {E, 0.0315789}, {S, 0.0263158}, {U, 0.0263158}, {Q, 0.0210526}, {L, 0.0157895},
 {C, 0.0105263}, {X, 0.0105263}, {I, 0.0105263}, {G, 0.00526316}}
```

$\boldsymbol{W_1}$ = {0.0126316, 0.0315789, 0.0105263, 0.0526316, 0.0315789, 0.0, 0.00526316 ...}

Vigenère Cipher - Find Key (Method #2)

- **Algorithm to find key of size *n*:**

For $j = 1$ to n, do the following:

1. Compute the frequencies of the letters in positions $j \pmod n$, and for the vector $\boldsymbol{W_i}$.
2. For $j = 1$ to 25, compute $\boldsymbol{W_i} \cdot \boldsymbol{A_j}$.
3. Let k_i be the maximum value of $\boldsymbol{W_i} \cdot \boldsymbol{A_j}$ over all $\boldsymbol{j}$, i.e.,

$$k_i = \max_{j \in [n]} \{W_i \cdot A_j\}$$

The key is probably $\{k_1, k_2, \ldots, k_n\}$.

- **Example**

```
W1 = {0.126, 0.032, 0.011, 0.053, 0.032, 0, 0.005,
   0.063, 0.011, 0.074, 0.116, 0.016, 0.000, 0.079, 0.042, 0.089,
   0.021, 0.000, 0.026, 0.00, 0.026, 0.000, 0.074, 0.011, 0.032, 0.063};
```

```
A0 = {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};
```

```
A1 = {0.001, 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};
```

```
Dot[W1, A1]
```

```
0.031351
```

Vigenère Cipher - Example

- **Dot Products:**

```
Table[Dot[W1, RotateRight[A0, j]], {j, 0, 25}]
```

```
{0.038829, 0.031351, 0.036403, 0.040457, 0.02872, 0.036892, 0.043885, 0.048653, 0.038415,
 0.043477, 0.037929, 0.041269, 0.035914, 0.03318, 0.034058, 0.036775, 0.0344, 0.034226,
 0.045895, 0.036622, 0.033637, 0.040424, 0.066214, 0.038061, 0.030079, 0.037237}
```

```
Table[Dot[W2, RotateRight[A0, j]], {j, 0, 25}]
```

```
{0.0346158, 0.0384474, 0.0320737, 0.0333632, 0.0462, 0.0343789,
 0.0291842, 0.0427105, 0.0661368, 0.0381053, 0.0300579, 0.0428789,
 0.0408, 0.0285947, 0.0360053, 0.0416842, 0.0294842, 0.0342579, 0.0405105,
 0.0415579, 0.0397421, 0.0450421, 0.0413632, 0.0423158, 0.0386526, 0.0328368}
```

```
Table[Dot[W3, RotateRight[A0, j]], {j, 0, 25}]
```

```
{0.035954, 0.031155, 0.033693, 0.044046, 0.03079, 0.038676, 0.038796, 0.033703, 0.035413,
 0.041124, 0.043312, 0.036802, 0.044546, 0.040496, 0.041534, 0.03453, 0.03209, 0.035455,
 0.039711, 0.03481, 0.033387, 0.046233, 0.035327, 0.031918, 0.039486, 0.067012}
```

```
Table[Dot[W4, RotateRight[A0, j]], {j, 0, 25}]
```

```
{0.067262, 0.036618, 0.030511, 0.038573, 0.045003, 0.030754, 0.035965, 0.037218, 0.033737,
 0.036613, 0.037828, 0.039671, 0.038791, 0.046443, 0.039421, 0.047947, 0.039017,
 0.034116, 0.029131, 0.039908, 0.033727, 0.0345, 0.044941, 0.033107, 0.029982, 0.041217}
```

```
Table[Dot[W5, RotateRight[A0, j]], {j, 0, 25}]
```

```
{0.042235, 0.042055, 0.046683, 0.035702, 0.043322, 0.03635, 0.040157, 0.036356, 0.031292,
 0.035165, 0.038063, 0.041698, 0.035241, 0.047897, 0.032617, 0.034907, 0.043524,
 0.062637, 0.032983, 0.029022, 0.038689, 0.038966, 0.03386, 0.033697, 0.039842, 0.031043}
```

```
Table[Dot[W6, RotateRight[A0, j]], {j, 0, 25}]
```

```
{0.035832, 0.033333, 0.038813, 0.065175, 0.037811, 0.031955, 0.034815, 0.042296, 0.031839,
 0.035198, 0.041335, 0.031554, 0.031681, 0.034127, 0.046489, 0.04066, 0.044773,
 0.036743, 0.045377, 0.041871, 0.034385, 0.03695, 0.04093, 0.03572, 0.026419, 0.044919}
```

- **Chapter 2 - Classical Cryptosystems**

Section 2.4 - Substitution Ciphers

Substitution Ciphers

In a **substitution cipher**, each alphabet letter is replaced with another (possibly the same) alphabet letter.

- **Examples**

- $\begin{pmatrix} \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} & \mathtt{g} & \mathtt{h} & \mathtt{i} & \mathtt{j} & \mathtt{k} & \mathtt{l} & \mathtt{m} & \mathtt{n} & \mathtt{o} & \mathtt{p} & \mathtt{q} & \mathtt{r} & \mathtt{s} & \mathtt{t} & \mathtt{u} & \mathtt{v} & \mathtt{w} & \mathtt{x} & \mathtt{y} & \mathtt{z} \\ \mathtt{B} & \mathtt{F} & \mathtt{K} & \mathtt{N} & \mathtt{Q} & \mathtt{X} & \mathtt{L} & \mathtt{Y} & \mathtt{H} & \mathtt{S} & \mathtt{R} & \mathtt{C} & \mathtt{D} & \mathtt{A} & \mathtt{I} & \mathtt{E} & \mathtt{J} & \mathtt{P} & \mathtt{Z} & \mathtt{G} & \mathtt{U} & \mathtt{O} & \mathtt{V} & \mathtt{W} & \mathtt{M} & \mathtt{T} \end{pmatrix}$
- Shift Ciphers
- Affine Ciphers

- **Weaknesses**

Substitutions can be attacked with frequency analysis.

- **Chapter 2 - Classical Cryptosystems**

Section 2.6 - The Playfair and ADFGX ciphers

The Playfair Cipher

- The Playfair system was invented around 1854 by Sir Charles Wheatstone who named it after his friend, Baron Playfair of St. Andrews.
- Used by the British during World War I and the Boer War.
- **Key Setup**

1. The *key* is a word: **snausages**
2. Delete repeated letters: **snauge**
3. Make a 5x5 grid starting with the key followed by the remaing alphabet letters (*i* and *j* are treated as the same letter):

s	n	a	u	g
e	b	c	d	f
h	i	k	l	m
o	p	q	r	t
v	w	x	y	z

- **Message Setup**

plaintext: beefy blurry line between snack time and a good time

- Remove spaces and divide the text into groups of two. Add in “x”s if blocks are the same. Pad last block with “x” if necessary:

  `be ef yb lu rx ry li ne be tw ex en sn ac kt im ea nd ag ox od ti me`

The Playfair Cipher

- Use the matrix to encode:

  1. If the two letters are not in the same row or column: replace each letter by the corresponding letter that is in the same row and also in the same column as its paired letter.

  2. If the two letters are in the same row: replace each letter with the letter to its immediate right (wrap if necessary).

  3. If the two letters are in the same coumn: replace each letter with the letter immediately below it (wrap if necessary).

- Reverse the proceedure to decode.

- **Example**

s	*n*	*a*	*u*	*g*
e	*b*	*c*	*d*	*f*
h	*i*	*k*	*l*	*m*
o	*p*	*q*	*r*	*t*
v	*w*	*x*	*y*	*z*

plaintext: `be ef yb lu rx ry li ne be tw ex en sn ac kt im ea nd ag ox od ti me`

ciphertext: `CB BE WD RD QY YU MK SB CB PZ CV BS NA CK MQ KH CS UB US QV RE PM HF`

The Playfair Cipher

- **Weaknesses**

- Frequency analysis of two letter combinations:

1. `th`, `he`, `an`, `in`, `re`, `es`, `er` are very common
2. since both "`er`" and "`re`" are common in english, can guess corresponding letters

- Each letter has at most five corresponding cipher letters.

- Last few rows of the matrix are predictable

The ADFGX Cipher

- Used by the German army during World War I.
- Successfully attacked by French cryptanalyst Georges Painvin and the Bureau du Chiffre
- **Key Setup**

1. Randomly arrange the alphabet letters into a 5x5 grid (*i* and *j* same letter):
2. Label rows and columns with “ADFGX”:

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

3. Choose a key word with distinct alphabet letters:

key: `smiley`

The ADFGX Cipher

plaintext: `neverputasockinatoaster` key: `smiley`

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

- **Encryption**

1. Substitue each letter for the row and column letters. For example: n → XA, e → DG

codetext: XA DG XF DG FG DX FF DA AF AX XG FD GF DD XA AF DA XG AF AX DA DG FG

2. Arrange coded text into rows of a grid with the columns labled with the keyword

s	m	i	l	e	y
X	A	D	G	X	F
D	G	F	G	D	X
F	F	D	A	A	F
A	X	X	G	F	D
G	F	D	D	X	A
A	F	D	A	X	G
A	F	A	X	D	A
D	G	F	G		

3. Alphabetize the columns

4. Encrypted message is formed from reading the columns