Playfair Cipher 9/5/2025

Sunday, August 24, 2025 1:35 PM

Quiz 1 tested what we call "monoalphabetic ciphers" --> one for one letter substitutions. (Shift, Affine, Substitution, Vigenere)

Maybe we substitute for more than one letter at a time--> let's do pairs…

Goals from Playfair's view:

1. Do something more complicated than substituting for each letter one by one
2. Do something that is easy to remember the key and execute both ways (encryption and decryption)

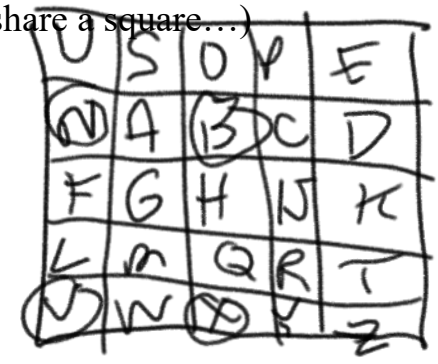
How it works:

1. Split the plaintext into pairs. If a pair has a double letter, then insert a padding character ('X'). (In the worst case, if the regular padding character is the double letter, then you need a backup padding character.) For our class let's agree to use 'X' and then if necessary 'Q' as the backup to 'X'. Only insert as needed as you go, so if you insert one padding character, then a future double letter, might not be in the same pair any more.
2. For each pair, encrypt using the playfair square.

How to form the playfair square:

1. Pick a secret keyword.
2. Fill out that keyword, removing any duplicate letters in a 5 by 5 square from top to bottom, left to right. Then fill in all other letters in order.

Key = "USOPEN" (Note: 5 x 5 = 25 25 but there are 26 letters, so I/J always share a square…)



How to encrypt:

If a pair of letters is on the same row, then substitute each letter, with the letter to the right. If there is no letter on the right, wrap around to the beginning (all the way left)

If a pair of letters is on the same column, then substitute each letter, with the letter below it. If there is no letter below, wrap around to the beginning (top)

If a pair of letters forms a diagonal of a rectangle, then encrypt each letter with a letter from the same row, but at the opposite corner of the rectangle.

Plaintext: "TENNISCHANNELSHOWSTENNIS"

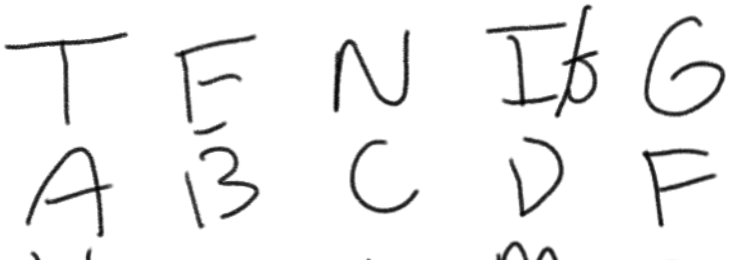
TE --> ZD (same column look below)
NX --> BV (box rule, also we padded with X to avoid NN)
NI --> CF (box rule)
SC --> PA (box rule)
HA --> BG (box rule)
NX --> BV (box rule)
NE --> DU (box rule)
LS --> MU (box rule)
HO --> QB (column rule look below)
WS --> SA (column rule with wrap around for encryption of W)
TE --> ZD
NX --> BV
NI --> CF
SX --> WO

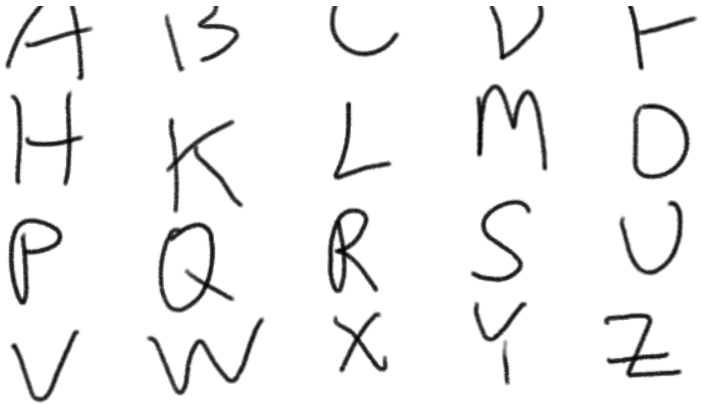
Row rule never came up, but if we had the pairs:

CA --> DB
ES --> UO

Example of removing duplicate letters:

Keyword: TENTING





To Decrypt:

For two letters on the same row, look to the left with a wrap around to the right most item on the row.

For two letters on the same column, look above with a wrap around to the bottom.

Box rule: Decryption is identical to encryption.

Breaking Playfair

Step One is recognizing that a text was encrypted with playfair.

Some commonalities of Playfair ciphertexts:

1. Always an even length.
2. Never any double letters in the cipher text.
3. Rare consonants (K, J, W, X, Y, Z) come up a lot.
4. Frequency distribution of digraphs approximates plaintext digraphs.

Other properties of Playfair

1. A letter never encrypts as itself.
2. Two reversed digraphs in the ciphertext are also reversed digraphs in plaintext.
3. Every letter can only be substituted by five other letters (any of the other letters on its row, or the letter below it with wrap around)

Typically, Playfair is a little harder to break than Vigenere. Often times, it's helpful to have some small amount of matching plaintext and ciphertext.

Plaintext: MI DN IG HT
Ciphertext: UG GK DH DA

Plaintext: MI DN IG HT
Ciphertext: UG GK DH DA

MI encrypts to UG…same row, or same col or box rule