|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Simple Substitution Cipher  **Description**  A monoalphabetic, or simple substitution, cipher is one in which the ciphertext alphabet is a rearrangement of the plaintext alphabet. Substitution ciphers, despite having 26! possible permutations, are actually very insecure and are easily solved  using letter frequencies. As Thomas Barr explains, “They are analogous to the cheap locks that sometimes come with luggage: a deterrent to the casual intruder but not to someone with even modest intentions of breaking in.” (Invitation to Cryptology, 84). Simple substitutions are a great way to encipher messages that need to be visually enciphered but easily deciphered.  **Example, Mixed Alphabet with Keywords**  The sender and receiver decides up on a keyword or phrase. In this case, let’s use the phrase “the cows go moo in the field.” The plaintext and ciphertext are laid out, with the key being made from the distinct letters of the key phrase:   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | plaintext | 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 | | ciphertext | T | H | E | C | O | W | S | G | M | I | N | F | L | D | A | B | J | K | P | Q | R | U | V | X | Y | Z |   The first half of the ciphertext letters were mapped  via the key phrase (omitting any repeated letters), and the second half was created by using the remaining letters of the alphabet in order from A to Z.  **Encipher** The sender enciphers the message MEET ME AT FIVE O’CLOCK for the receiver to decrypt. To encipher this message, simply line up each plaintext letter from the message with the ciphertext letter in the chart.   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | plain |  | cipher |  | plain |  | cipher | | M |  | L |  | V |  | U | | E |  | O |  | O |  | A | | T |  | Q |  | C |  | E | | A |  | T |  | L |  | F | | F |  | W |  | K |  | N | | I |  | M |  |  |  |  |   This gives the enciphered message LOOQLOTQWMUOAEFAEN  **Decipher** Since the receiver knows the key phrase, they can set up the above chart just like the sender di, and easily decrypt the enciphered message.   |  |  |  | | --- | --- | --- | | cipher |  | plain | | L |  | M | | O |  | E | | Q |  | T | | ... |  | ... | | F |  | L | | N |  | K |   This gives the deciphered message MEETMEATFIVEOCLOCK    **Disadvantage**  The major problem with simple substitution ciphers is that the frequencies of letters are not masked at all. If the enciphered message LOOQLOTQWMUOAEFAEN was intercepted, the interceptor could look at the frequencies of each letter and compare them to the frequencies of English: 'O' is used four times in the enciphered message, and L, Q, A, and E all appear twice. The top nine letters for English frequencies are E, T, A, O, N, I, S, R, and H. As a guess, the interceptor could line up the letters as follows:   |  |  |  | | --- | --- | --- | | cipher |  | plain | | O |  | E | | L |  | A | | Q |  | T | | A |  | O | | E |  | N |   A quick deciphering test gives the answer AEETAE?T???EON?ON? If the interceptor agrees that O = E and sees that the first phrase could decipher as MEET ME AT then they would have an easy time deciphering the rest of the message. | |
|  |