Cryptography

Why Encryption Matters

- Networks are open to everyone, so we assume that anyone may acquire messages sent across networks

- You don’t want your messages read, but there is little that can be done if some REALLY wants to read them (especially if it’s on a network)

- What can we do to stop them from reading messages, even if we assume they can acquire the message?
  - Encrypt the message so that it still can’t be read (at least, not without decrypting it first)

Needs for Cryptography

- Top secret or protected communication
  - Government/Company secrets
  - War strategies and information
  - Email
  - Bank transactions
  - etc.

- Cryptography is nothing new, the oldest known use is around 1900 B.C.E in Egypt

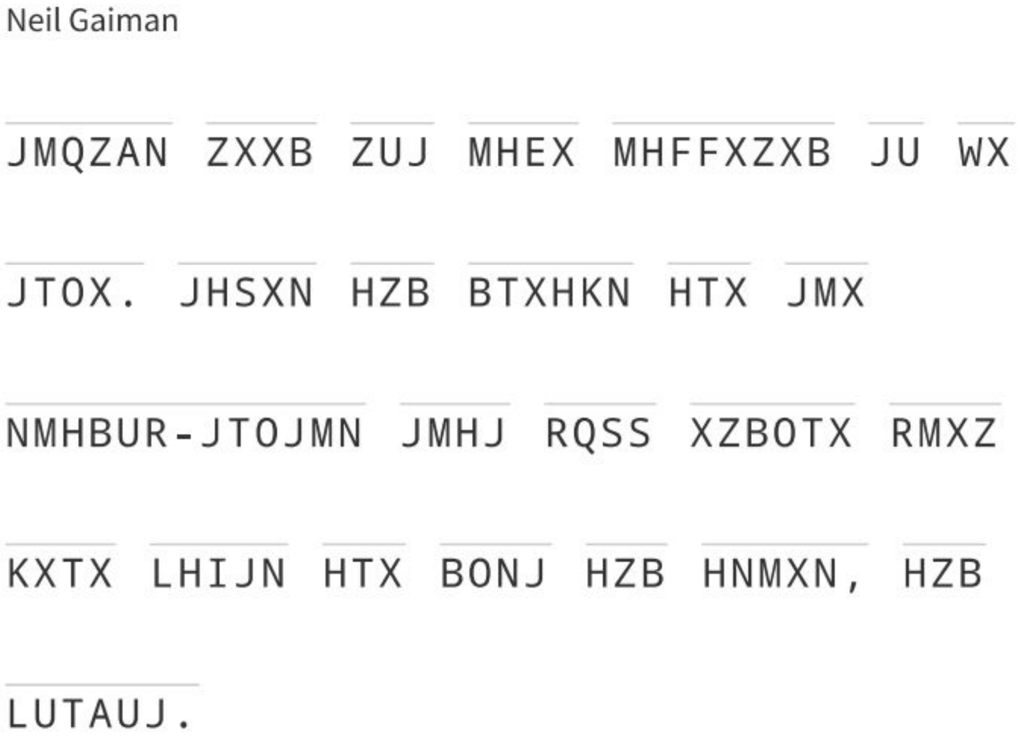
- What does it mean for something to be secure?
  - Claude Shannon; Shannon Cipher: An attacker can do no better than random guessing

Ciphers/Cyphers

- Symmetric cryptography (private-key)
  - Uses the same key to encrypt and decrypt
  - Substitution
    - Hello World => noppq vqjpe
  - Transposition
    - Hello World => elwodhrllo
  - Polyalphabetic Substitution
    - Hello World => tjyad itear (adding “lemon” to letters)
    - Hello World => sixzb hsdzq (Vigenère Cipher using “lemon”)

- Public-key (Asymmetric cryptography)
  - Uses different keys to encrypt and decrypt

In-Class Activity: Cryptogram



Neil Gaiman

JMQZAN ZXXB ZUJ MHEX MHFFXZXB JU WX

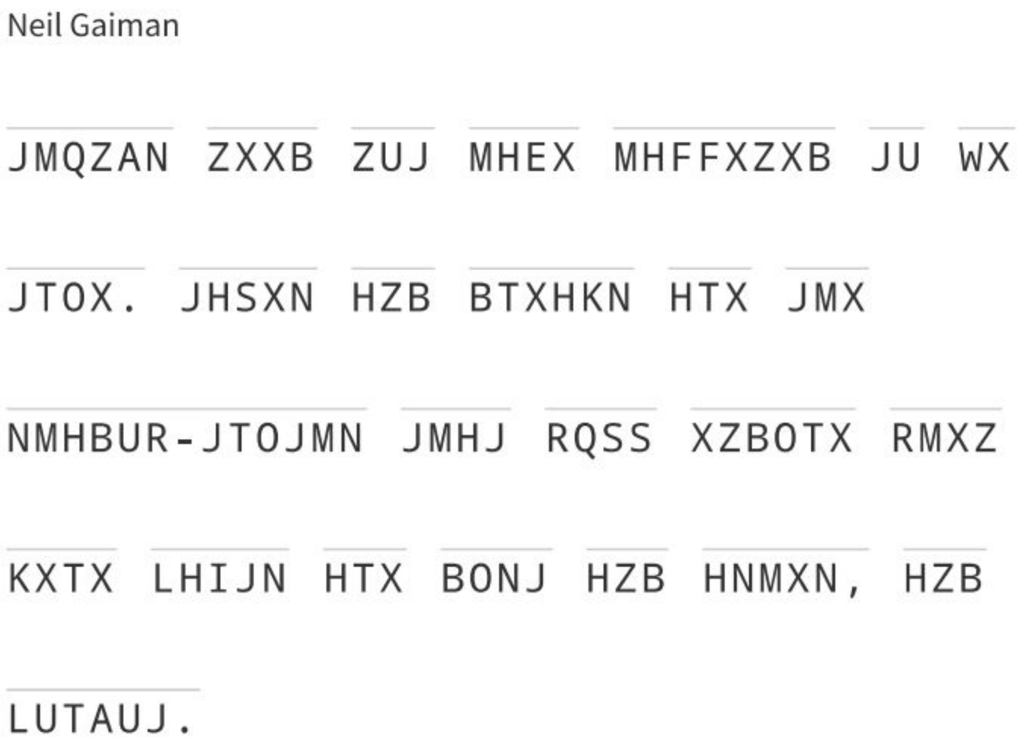
JTOX. JHSXN HZB BTXHKN HTX JMX

NMHBUR-JTOJMN JMHJ RQSS XZBOTX RMXZ

KXTX LHIJN HTX BONJ HZB HNMXN, HZB

LUTAUJ.

In-Class Activity: Cryptogram



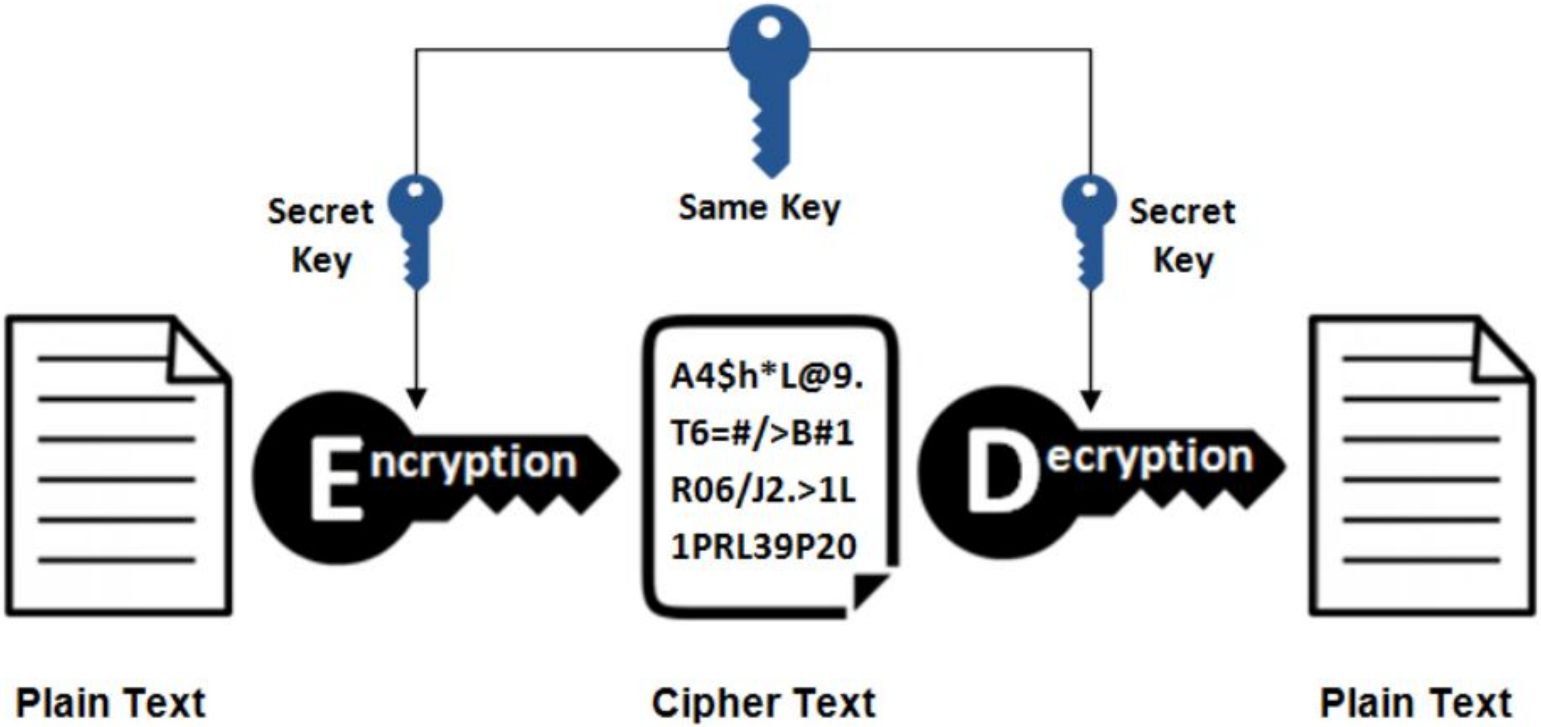
Neil Gaiman

JMQZAN ZXXB ZUJ MHEX MHFFXZXB JU WX
JTOX. JHSXN HZB BTXHKN HTX JMX
NMHBUR-JTOJMN JMHJ RQSS XZBOTX RMXZ
KXTX LHIJN HTX BONJ HZB HNMXN, HZB
LUTAUJ.

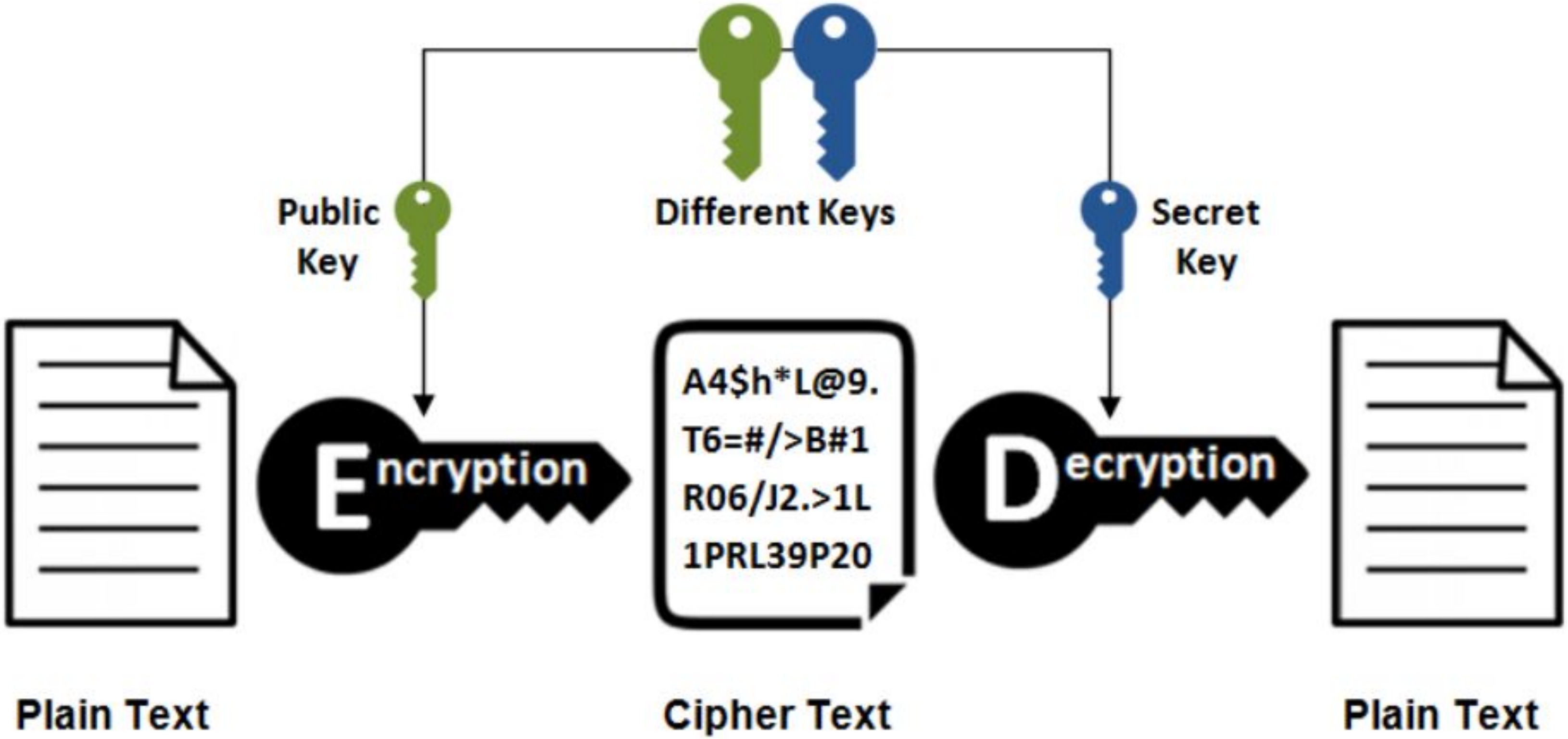
Character Frequency:
X - 18
J - 13, H - 13
M - 9, N - 9, Z - 9, B - 9
T - 8
U - 5
O - 4
S - 3, R - 3
Q - 2, A - 2, F - 2
E - 1, W - 1, I - 1

- ‘E’ is the most common letter in the English language
- Frequency depends on the type of analysis (‘A’ or ‘T’ is often the next most common letters)

Symmetric Encryption



Asymmetric Encryption



RSA Encryption (Asymmetric Encryption)

- RSA (Rivest–Shamir–Adleman) Encryption

- Mathematics of Algorithm:
  - Select 2 prime numbers p and q (p = 53, q = 59)
  - **Public Key, (n,e)**:
    - n = p*q (n = 3127)
    - e is a small exponent that must NOT be a factor of n (so must not be p or q) and must be 1 < e < (p-1)(q-1) (1 < e < 3016; e = 3)
  - **Private Key, (d,e)**:
    - d = (k * (p-1)(q-1) + 1) / e, for some integer k (k = 2; d = 2011)
  - To Encrypt: m^e mod n (where m is the message)
  - To Decrypt: c^d mod n (where c is the cipher)

  - Try for “HI” = 89

RSA Encryption (Asymmetric Encryption)

- Relies on the fact that it is difficult to factor large numbers (i.e., find the prime factorization)

- Relies on the size of the public/private keys
  - We need two BIG prime numbers (typically 1024 bits today (i.e., about 1.8 x 10^{308} in decimal) but there is a growing move to 2048 bits)