ATTACK AT 1200 AM
36 = 26 + 10

AD DD DD AD AG VG AD DD AF DG VF VF AD DX
LETTERS DIGITS

Step 1: Do substitution by chart.
Randomly fill square with all 36 chars.

Step 2: Keyword (PRIVACY)

PRIVACY
ADD JDDD A

DAGVGA D
DADFEGV

FOOTBALL

Transposition

Read in the order of the #s of the columns:

DGDDDA6DG6A

ADDFAADV DVFA ADVX

Msglen = 30/7 = 4 (4 or 5)
30%7 = 2 (# cols that are 5)
THIS IS A SHORT MESSAGE

Chair

This is a short message.

SASHO RTMES SAGE

ISMGTSR$HATASHEEIOS

THIS I SAOHS RTSEM SAGE

THISI SASHO RTMES SAGE

Keep Take Home MSGs

Combination of 2 different ciphers into one can make a stronger cipher than either system.

Claude Shannon → Substitution, Confusion + Diffusion → the effect of a single plaintext spreads letter to multiple places in the ciphertext.
Composing Ciphers

1. Substitution followed by substitution?
   \[ A \rightarrow Q \rightarrow B \leftrightarrow A \rightarrow B \]

2. Affine followed by affine?
   Produces another valid affine (no better)

3. Vigenère followed by Vigenère?

   AGEAGEAGEAGEAGEAGE
   FRUITFRUITFRUIT

   Effect is on a Vigenère with keyword length 1 cm \((a, b)\), where \(a, b\)
   are the lengths of the 2 keywords.
   Order of adding does not matter.