Cryptography 4 Worksheet: Double Transposition

Double Transposition

1. Use first keyword `SHIP` and second keyword `ARTEMIS`, to encrypt the phrase

   THE LAUNCH IS A GO

HLOTN HEAUC SGIA

2. What would happen if the keyword SHIP was replaced with the keyword MOON?

   Exactly how to order the two O's is a little bit ambiguous. Presumeably, one would not reorder those columns but ... one could choose to do so...

3. What would happen if the keyword SHIP was replaced with the keyword FLOP?

   FLOP is already in alphabetical order ... So no re-ordering happens

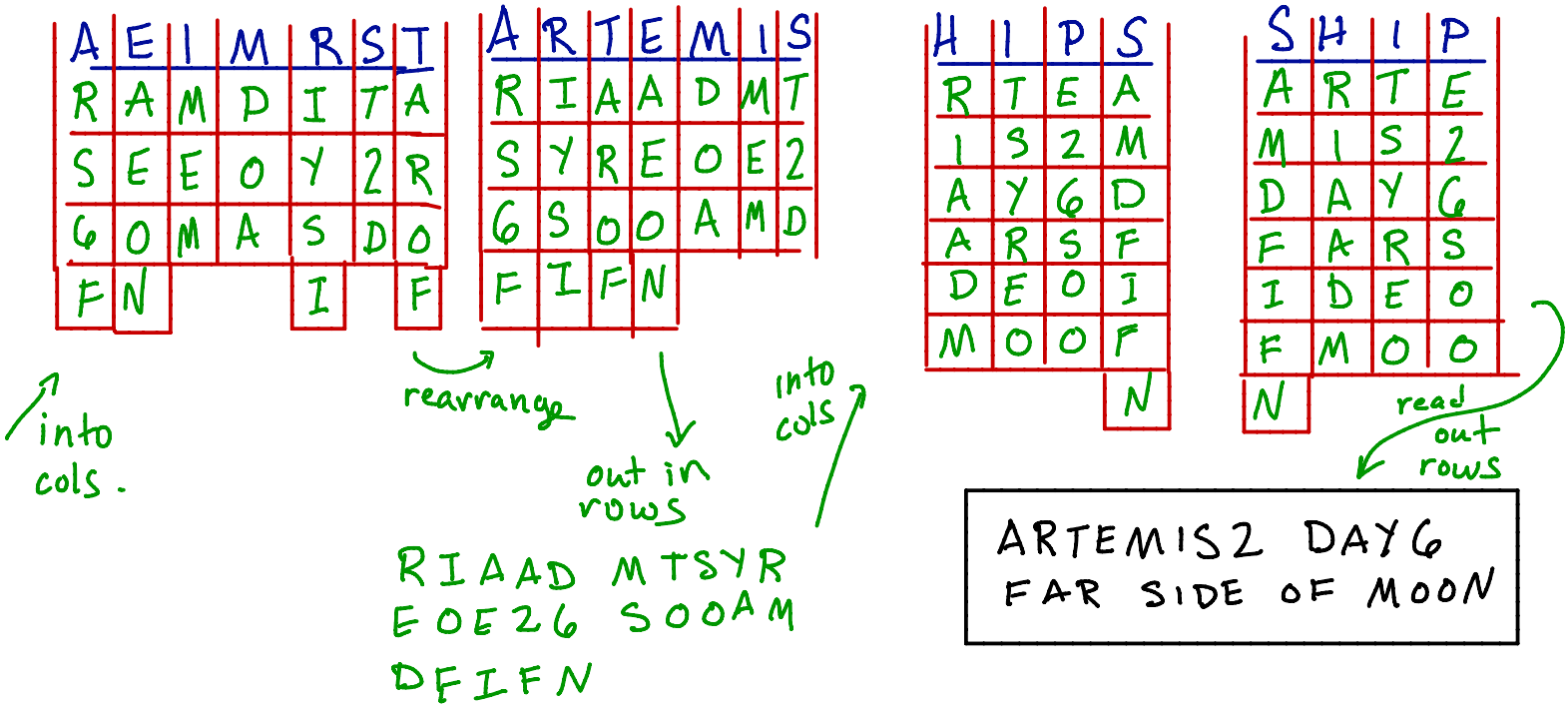
4. What might you want in a good keyword?

   - No repeated letters avoids ambiguity
   - Words with letters NOT in alphabetical order.

5. Assuming the ciphertext was encrypted using double transposition with first keyword SHIP and second keyword ARTEMIS, decrypt the ciphertext.

   RS6FA EONME MDOAI YSIT2 DAROF

grid calculations # letters in ciphertext: 25
SHIP : 4
ARTEMIS : 7
"SHIP" grid: $\frac{25}{4} = 6R1$
"ARTEMIS" grid: $\frac{25}{7} = 3R4$



RIAAD MTSYR
EOE26 SOOAM
DFIFN

ARTEMIS2 DAY6
FAR SIDE OF MOON

6. What are some advantages of a double transposition cipher?

- Very scrambled.
- Used in WWII on both sides. Pretty secure provided keys keep changing. (Not so much now...)

7. What are some disadvantages of a double transposition cipher?

Requires careful rewriting.
Better for longer rather than shorter messages which can be unscrambled by inspection.