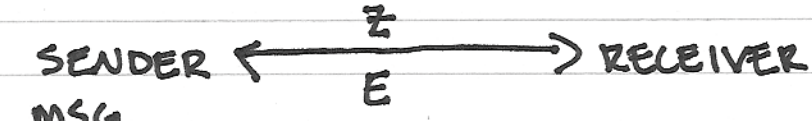
RYAN
ROMANOWSKI

2/16

GREEDY ALGORITHMS
- VERY INTUITIVE
- FOR SOME ALGORITHMS, LESS OPTIMAL
- YOU'RE ABLE TO REDUCE THE PROBLEM SIZE
  ↳ SUB STRUCTURE OPTIMALITY → INDUCTION

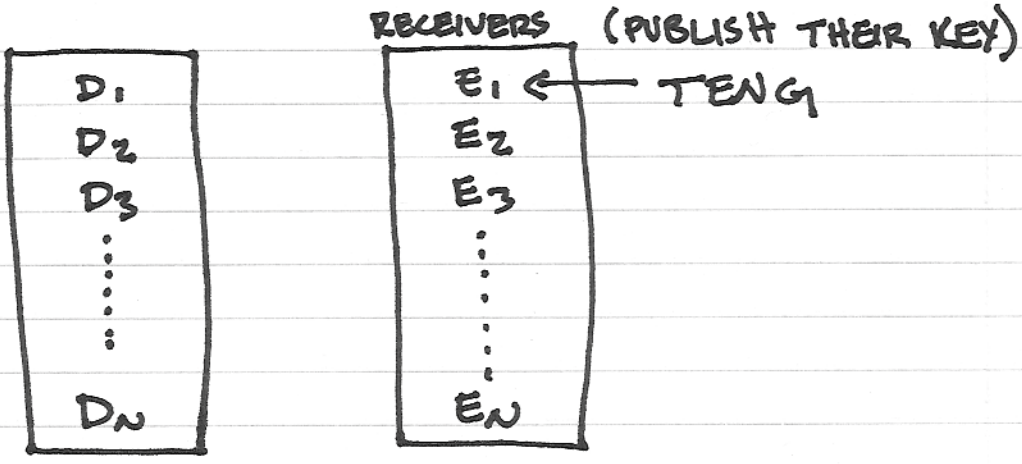
KNAPSACK PROBLEM (SPECIAL CASE)
INPUT: $w_1, w_2, w_3, \ldots, w_n, K$
(OBJECTS) (CAPACITY OF KNAPSACK)
OUTPUT: $S \subseteq \{1, 2, \ldots, n\}$
WANT TO OUTPUT A SUBSET SUCH THAT $\sum_{i \in S} w_i = K$
→ ITEMS AREN'T DIVISIBLE

ENCRYPTION (WHICH REALLY ADVANCED COMPUTER ALGOS)



...BUT IF THE SENDER AND RECEIVER HAVEN'T TALKED YET, HOW CAN THEY SHARE A SECRET, PRIVATE LANGUAGE?
↳ PUBLIC KEY ENCRYPTION SCHEME

"YELLOW BOOK ENCRYPTION SCHEME"



→RSA IS A VARIATION OF THIS

MERKLE-HELLMAN (STANFORD)
↳ HAS BEEN BROKEN

$\alpha_1, \alpha_2, \ldots, \alpha_n$ $\quad \alpha_i = 1$ IFF $n \in S$
$\alpha_i = 0$

$m = (m_1, m_2, \ldots, m_n)$

ENCRYPTION
1) CHOOSE $(W_1, W_2, \ldots, W_n)$ SUCH THAT FOR ALL i

$$W_i > \sum_{j=1}^{i-1} W_j \quad \text{(SUPERINCREASING)}$$

↳ NEXT NUMBER > SUM OF PREVIOUS 2 NUMBERS

$(2, 7, 11, 21, 42, 89, 180, 354)$ $\quad \sum_i = 706$

2) CHOOSE LARGE RANDOM q SUCH THAT $q > \sum_{i=1}^{n} W_i$
$q = 881$

3) CHOOSE A LARGE RANDOM r SUCH THAT
$GCD(r, q) = 1$
$r = 588$

4) ENCRYPTION KEY $(\beta_1, \beta_2, \ldots, \beta_n)$ SUCH THAT
$\beta_i = r w_i \bmod q$

→ THIS MAKES IT SEEM RANDOM

(295, 592, 301, 14, 28, 353, 120, 236)
↳ YELLOW PAGE ENTRY

5) PUBLISH $(\beta_1, \beta_2, \ldots \beta_n)$ PUBLIC
KEEP $(w_1, w_2, \ldots w_n), q, r$ PRIVATE

ENCRYPTION:
- MESSAGE = 01100001
- PAIRWISE MULTIPLY W/ YELLOW PAGE ENTRY
$592 + 301 + 236 = 1129$ (CIPHERTEXT)

DECODING:
- JUST A KNAPSACK PROBLEM
... BUT KNAPSACK PROBLEM'S HARD ...

ONEWAY-NESS
→ EASIER TO ENCODE, SEEMINGLY HARD TO DECODE

KNAPSACK PROBLEM FOR SUPERINCREASING SEQUENCES:
→ GREEDY

$W = (2, 7, 11, 21, 42, 89, 180, 354)$ $K = 372$

0 1 1 0 0 0 0 1

$372 - 354 = 18$

$18 - 11 = 7$

$7 - 7 = 0$

-TAKE THE LARGEST ONE YOU CAN

-WHERE DID 372 COME FROM?

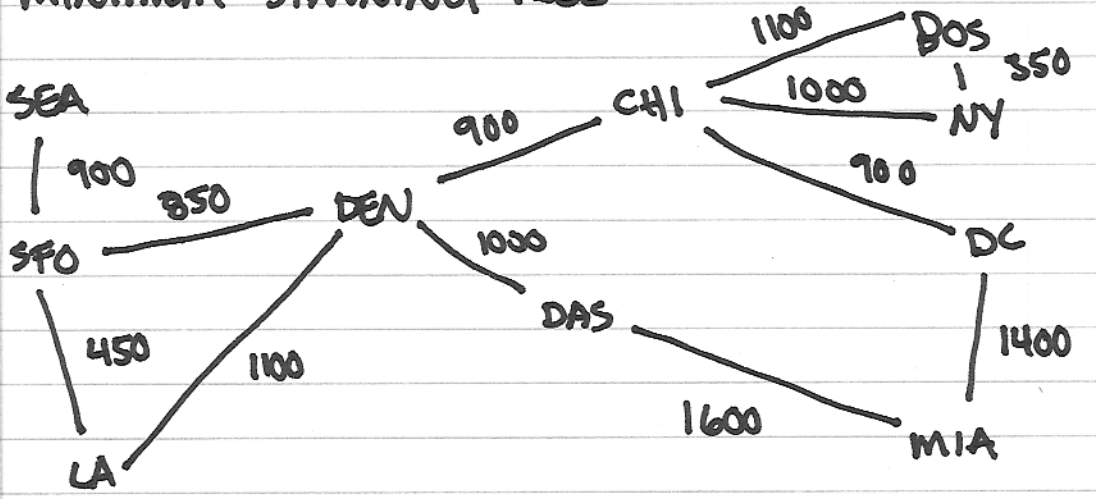
$q = 881$ $r = 588$ $s = 442$

$GCD(q, r) = 1$ $\exists\ s,\ s \cdot R = 1 \bmod q$

$1129 \cdot 442 \bmod 881 = 372$

THIS ALL FAILED AFTER SHORTEST VECTOR PROBLEM WAS SOLVED (UNRELATED PROBLEM)

MINIMUM SPANNING TREE



GIVEN THIS MAP, FIND A TREE CONNECTING ALL CITIES WITH THE SHORTEST TOTAL LENGTH

- DIVIDE MAP INTO 2 PARTS, THEN THE SHORTEST DISTANCE BETWEEN 1ST & 2ND SETS BELONGS TO THE TREE

ALGORITHM 1
1) ORDER CITIES PAIRWISE BY DISTANCE
2) CONNECT SHORTEST
3) CONNECT NEXT SHORTEST UNTIL IT INDUCES A CYCLE
   ↳ THEN THROW AWAY THE LINK THAT CREATES THE CYCLE
4) CONTINUE UNTIL THE COUNTRY IS CONNECTED

ALGORITHM 2
1) PICK A STARTING CITY AND CONNECT ITS CLOSEST NEIGHBOR
2) CONNECT THE NEXT CLOSEST CITY TO THE GROUP
3) THAT CITY IS NOW PART OF THE GROUP
4) REPEATE STEP 2-3 UNTIL ALL CITIES ARE CONNECTED