The Puzzler's Elusion Revealed

Rose's Message

The hint in the newspaper clipping ("Rove should have played fair.") and the hint on the post-it note ("present tense") suggest a Playfair cipher with a keyword of "ROVE":

R	O	V	E	A
B	C	D	F	G
H	I/J	K	L	M
N	P	Q	S	T
U	W	X	Y	Z

Below, Rose's encrypted message as it appeared in the newspaper is reproduced:

```
fvro lfkyijexu ijppmyapt
  mp lp lz ijrso nmgz bv ofwdaw opkymy
fvbowsza nmlp sfqzsaau clenza
  nmay grkyijent mw mrea hp lz wcqyy-
fqyplrp yooa uootwqvf wn hp ga todijg-
may hp ga bxijttnao prza geau beaij lvzu
payoau hp fijaefsrtgx uijzu mw cv prza
hqco aeao plpbay faqzpmtb nmal mw mrea
fryvtu nwenyrgx fu socwsf opnlhpma pa
cv la mrah
  hp vofvau pa sfza nmay grkyijent yfyv
nmay mkbmza ec gvzu mw sakymy wewu
nmfe hp rpay ec pzaw sijogfy nmfe roay
vyogsmzu ga foanomtu urhgao ec hksfty
peznmu rtgx pzaw hksfty yotn ec nmay
rsnartfo pa nmay nwfhpij mkhbrozu hp
ijrwvgx oheaau nmgz foanomtu urhgao lp
nmay rtpyao pa nmay bijemykrsfa norcsfta
ec nmay zovuohvoty ec orqnrbay nwuyy-
may hp noecfyyqvo pfrosfza ty trvuorp-
mea ijewvmx rorwqb clqb nmay meabvyfyza
wpsr rtgx ckma nmaoay nmay urhgao ec
lfyvza wewu ckma lp nmay rtpyao pa
nmay bijemykrsfa norcsfta ec nmay uijgz
ijcijeau lp lz mrza nwuyymay lc nmgz
cvfytu za ocvh nazu ga foanomtu urhgao
ec hksfty artn ec nmay ortbao tngzpctu
rp nmay eijgx ijkbmzozu artn ec ijrwvgx
oheaau rtgx ca wn pzrssz lfyvza nmgz
foanomtu urhgao lp nmay rtpyao pa nmay
bijemykrsfa norcsfta ec sehpma pedijty
ijewvmx ceau nmay hwphsoau
  ovyf vfzovbty
```

Unlike a traditional Playfair cryptogram, this message contains spaces that separate blocks of text. Several of the blocks are repeated many times. For instance, look for the block, "`nmay`". It appears the most often. Repeats of chains of blocks can also be found, such as, "`lp nmay rtpyao pa nmay bijemykrsfa norcsfta ec`". Both of these facts suggest that each block is an individually encrypted word.

It's also unusual for a Playfair cryptogram to contain all the letters of the alphabet since the key table has only 25 spaces. However, in this case, "`i`" is always paired with "`j`". To make it easier to decrypt, here's the message with the j's removed:

```
fvro lfkyiexu ippmyapt
  mp lp lz irso nmgz bv ofwdaw opkymy
fvbowsza nmlp sfqzsaau clenza
  nmay grkyient mw mrea hp lz wcqyy-
fqyplrp yooa uootwqvf wn hp ga todig-
may hp ga bxittnao prza geau beai lvzu
payoau hp fiaefsrtgx uizu mw cv prza
hqco aeao plpbay faqzpmtb nmal mw mrea
fryvtu nwenyrgx fu socwsf opnlhpma pa
cv la mrah
  hp vofvau pa sfza nmay grkyient yfyv
nmay mkbmza ec gvzu mw sakymy wewu
nmfe hp rpay ec pzaw siogfy nmfe roay
vyogsmzu ga foanomtu urhgao ec hksfty
peznmu rtgx pzaw hksfty yotn ec nmay
rsnartfo pa nmay nwfhpi mkhbrozu hp
irwvgx oheaau nmgz foanomtu urhgao lp
nmay rtpyao pa nmay biemykrsfa norcsfta
ec nmay zovuohvoty ec orqnrbay nwuyy-
may hp noecfyyqvo pfrosfza ty trvuorp-
mea iewvmx rorwqb clqb nmay meabvyfyza
wpsr rtgx ckma nmaoay nmay urhgao ec
lfyvza wewu ckma lp nmay rtpyao pa
nmay biemykrsfa norcsfta ec nmay uigz
icieau lp lz mrza nwuyymay lc nmgz
cvfytu za ocvh nazu ga foanomtu urhgao
ec hksfty artn ec nmay ortbao tngzpctu
rp nmay eigx ikbmzozu artn ec irwvgx
oheaau rtgx ca wn pzrssz lfyvza nmgz
foanomtu urhgao lp nmay rtpyao pa nmay
biemykrsfa norcsfta ec sehpma pedity
iewvmx ceau nmay hwphsoau
  ovyf vfzovbty
```

In this form, every block has an even number of characters and when those blocks are broken into digraphs, no double-letter diagraphs are found. Both of these are requirements for Playfair decryption.

The indentation suggests that the message is formatted like a letter. Since it originated from Rose Edwards, it might be of this form:

```
Dear [SOME NAME]
[PARAGRAPH 1]
[PARAGRAPH 2]
[PARAGRAPH 3]
  Rose Edwards
```

Continuing with that assumption, here's a comparison of those 3 encrypted blocks and their proposed decryption:

`Dear Rose Edwards`
`fvro ovyf vfzovbty`

The word, "Edwards", contains an odd number of characters. In accordance with Playfair encryption, which acts on digraphs, a padding character needs to be appended. The padding character is typically an infrequently used symbol, such as "Q" (which rarely appears at the end of English words) or "X" (which is just infrequently used). Padding it with a "?", makes the proposed decryptions line up. Here's what it looks like after breaking it into digraphs and dropping case:

`de-ar ro-se ed-wa-rd-s?`
`fv-ro ov-yf vf-zo-vb-ty`

Using the key table above, the pairs match up perfectly. Reversing "`ty`" produces "`sz`":

`de-ar ro-se ed-wa-rd-sz`
`fv-ro ov-yf vf-zo-vb-ty`

Decrypting the first line of the message yields:

`dear felxlowz citizens`
`fvro lfkyiexu ippmyapt`

In addition to a padding character, Playfair encryption requires a character to break up double-letter diagraphs in the source text. From the word, "`felxlowz`" (fellow), it appears that the double-letter diagraph separator is "`x`" and as mentioned above, the padding character is "`z`".

Here's the fully decrypted message:

```
dear felxlowz citizens
fvro lfkyiexu ippmyapt

  it is my hope that dr ecxcoz wilxlz
  mp lp lz irso nmgz bv ofwdaw opkymy

decryptz this letxterz firstz
fvbowsza nmlp sfqzsaau clenza

  thez balxlots iz have in my posxs-
  nmay grkyient mw mrea hp lz wcqyy-
```

esxsion were wrapxped up in az packa-
fqyplrp yooa uootwqvf wn hp ga todig-

gez in az dumpster notz farz from keyz
may hp ga bxittnao prza geau beai lvzu

towerz in clevelandz whyz iz do notz
payoau hp fiaefsrtgx uizu mw cv prza

know ever sincez getxting them iz have
hqco aeao plpbay faqzpmtb nmal mw mrea

bexenz pursuedz by people wishingz to
fryvtu nwenyrgx fu socwsf opnlhpma pa

do me harm
cv la mrah

in orderz to letz thez balxlots sexe
hp vofvau pa sfza nmay grkyient yfyv

thez lightz of dayz iz telxlz youz
nmay mkbmza ec gvzu mw sakymy wewu

they in onez of twoz places they arez
nmfe hp rpay ec pzaw siogfy nmfe roay

exactlyz az certainz number of milesz
vyogsmzu ga foanomtu urhgao ec hksfty

southz andz twoz milesz west of thez
peznmu rtgx pzaw hksfty yotn ec nmay

entrance to thez public libraryz in
rsnartfo pa nmay nwfhpi mkhbrozu hp

hoxodz riverz that certainz number is
irwvgx oheaau nmgz foanomtu urhgao lp

thez answer to thez chalxlenge problemz
nmay rtpyao pa nmay biemykrsfa norcsfta

of thez warxriorsz of rapturez puzxz-
ec nmay zovuohvoty ec orqnrbay nwuyy-

lez in profesxsor scarletz sz narxrat-
may hp noecfyyqvo pfrosfza ty trvuorp-

ive loxokz around find thez largexestz
mea iewvmx rorwqb clqb nmay meabvyfyza

pine andz digz therez thez number of
wpsr rtgx ckma nmaoay nmay urhgao ec

fexetz youz digz is thez answer to
lfyvza wewu ckma lp nmay rtpyao pa

thez chalxlenge problemz of thez what
nmay biemykrsfa norcsfta ec nmay uigz

colorz is my hatz puzxzlez if that
icieau lp lz mrza nwuyymay lc nmgz

doesnz tz work tryz az certainz number
cvfytu za ocvh nazu ga foanomtu urhgao

of milesz east of thez ranger stationz
ec hksfty artn ec nmay ortbao tngzpctu

on thez oldz highwayz east of hoxodz
rp nmay eigx ikbmzozu artn ec irwvgx

riverz andz go up twenty fexetz that
oheaau rtgx ca wn pzrssz lfyvza nmgz

certainz number is thez answer to thez
foanomtu urhgao lp nmay rtpyao pa nmay

chalxlenge problemz of lyingz socksz
biemykrsfa norcsfta ec sehpma pedity

loxokz forz thez iuniperz
iewvmx ceau nmay hwphsoau

rose edwardsz
ovyf vfzovbty

A few things to note: First, since the decryption omitted "j" in the key table, a few words require some i-to-j conversions. For instance, the last word of the final paragraph is probably "juniper". Second, four words in the message are wrapped around onto the next line via a hyphen. The decryption treated hyphenated blocks as a single block without the hyphen. Third, aside from obviously missing punctuation, apostrophes in the original message apparently were treated as a space separating blocks. For instance:

doesnz tz
cvfytu za

Above, "doesn't" is shown decrypted. Note that it was split into 2 blocks and each block was padded independently with "z". Finally, one word has a strange spelling:

largexestz
meabvyfyza

Normally, the word, "largest", contains only one "e". Note that this word contains 2 syllables and it appears at the end of the line. It is possible that Rose originally hyphenated the word to wrap it onto the next line at which point an extra "e" was introduced: large-est. During editing, perhaps the word was unwrapped, but the extra "e" was inadvertently left there. Though, this is complete speculation.

Compensating for the lack of case and punctuation and the things noted above results in this translation:

> Dear Fellow Citizens,
>
> It is my hope that Dr. Ecco will decrypt this letter first.
>
> The ballots I have in my possession were wrapped up in a package in a dumpster not far from Key Tower in Cleveland, why I do not know. Ever since getting them, I have been pursued by people wishing to do me harm.
>
> In order to let the ballots see the light of day, I tell you, they [are] in one of two places. They are exactly a certain number of miles south and two miles west of the entrance to the public library in Hood River. That certain number is the answer to the challenge problem of the *Warriors of Rapture* puzzle in Professor Scarlet's narrative. Look around. Find the largest pine and dig there. The number of feet you dig is the answer to the challenge problem of the *What Color is my Hat* puzzle. If that doesn't work try a certain number of miles east of the ranger station on the old highway east of Hood River and go up twenty feet. That certain number is the answer to the challenge problem of *Lying Socks*. Look for the juniper.
>
> Rose Edwards

What if the hint in the newspaper simply read, "They should have played fair"? Meaning, what if the hint implied that the message was encrypted using a Playfair cipher, but the keyword was not provided? The keyword can actually be derived with a little guesswork.

In cryptanalysis, a "crib" is a portion of known or suspected plaintext. Three cribs were proposed above:

```
de-ar ro-se ed-wa-rd-s?
fv-ro ov-yf vf-zo-vb-ty
```

Note the following 2 encryption mappings: `ar` → `ro`, `ro` → `ov`. In the first, the letter "`r`" appears in both the plaintext and the encrypted digraph. This is only possible, if the key table contains the sequence, A R O, across a row or down a column (possibly wrapped around the key table). In the second mapping, the letter "`o`" appears in both. As with the first, this is only possible, if the key table contains the sequence, R O V, across a row or down a column. Since both sequences contain R O, the sequence A R O V must appear across a row or down a column.

Now, a Playfair key table contains only 5 rows and 5 columns, but consider the sequence A R O V written across a row on a large grid:

		A	R	O	V		

The cribs also provide the following mappings: `de` → `fv`, `ed` → `vf`. In this case, the second mapping could have been derived from the first because in a Playfair cipher, the mapping `AB` → `CD` implies `BA` → `DC`. There are 2 possible configurations that could enable `de` to map to `fv`. First, `d`, `e`, `f` and `v` may be in the same column (though there may be an extra space below F and above E):

					D		
					F		
					E		
		A	R	O	V		

Or, `d` is in the same column as `v`, and `e` is the fifth letter in the A R O V row. And, in that case, `f` must be in the same column as `e`:

					D	F	
					D	F	
					D	F	
		A	R	O	V	E	
					D	F	
					D	F	
					D	F	

The cribs also provide the mapping: `se` → `yf`. In the first case, `s`, `e`, `y` and `f` cannot be in the same column because there is only room for 5 letters in the real key table and `d`, `f`, `e` and `v` are already occupying 4 of them. That means the mapping exists because the four letters are oriented in one of these configurations

```
S . . . Y       E . . . F
.       .       .       .
.       .       .       .
.       .       .       .
F . . . E       Y . . . S
```

In both, `e` and `f` share the same row, which is a contradiction with the assumption that they share the same column. Hence, the sequence A R O V E must exist across a row or down a column (possibly wrapped) in the Playfair key table.

Now consider the 5 possible rotations of A R O V E:

```
AROVE
ROVEA
OVEAR
VEARO
EAROV
```

In none of them are the letters in alphabetical order. If the sequence represents a row, then it must contain at least part of the keyword. With that assumption, each rotation can be used to generate a unique key table by moving it to the top row and filling in the emptying spaces with the remaining letters of the alphabet in alphabetical order. One of them will decrypt the message properly.

What if the key table did not contain a keyword? Suppose it was a random jumble of letters. It is still possible to derive the complete key table with guesswork and trial-and-error.

Starting with the cribs above and taking into account the rule `AB` → `CD` implies `BA` → `DC`, digraph substitutions can be performed across the message. Consider the first line of the first paragraph:

```
?? ?? ?? ???? ???? dr ?????? ??????
mp lp lz irso nmgz bv ofwdaw opkymy
```

That `dr` must be short for doctor and hence, it's safe to assume that `ofwdaw` is Ecco:

```
?? ?? ?? ???? ???? dr ec?co? ??????
mp lp lz irso nmgz bv ofwdaw opkymy
```

As discussed above, to encrypt "Ecco" requires a double-letter diagraph separator and a padding character, both of which are initially unknown.

For the mapping `AB` → `CD`, if `A` and `B` are not in the same row or column, then `AB` → `CD` implies `CD` → `AB`. Since `e` and `f` are not in the same row as discussed above, the word `of` maps to `ec`.

Next, consider this phrase:

??ofes??or ??ar???? s?
noecfyyyqvo pfrosfza ty

It's not difficult to guess that this is:

profes?sor scarlet?'s?
noecfyyyqvo pfrosfza ty

Continuing, since "nmay" appears more often than any other encrypted word, it's safe to assume that it is "the":

the?
nmay

After several nearby words are decrypted, it is often possible to fill in the missing words by analyzing the context of the sentence. It is also helpful to read ahead in the book about the actions Dr. Ecco carried out in response to decrypting the message. For example, after decrypting the word, "river", it is safe to assume it is preceded by, "hood".

Repeatedly applying these ideas and making many guesses perhaps with the aid of an online crossword puzzle dictionary will ultimately decrypt most of the message. The double-letter diagraph separator and the padding character can be derived from these words:

citizens
ippmyapt

exactly?
vyogsmzu

Some of the words are almost impossible to decrypt without deriving the key table, such as this one:

??ne
wpsr

There are plenty of four-letter words ending in "ne" and "wp" appears no where else in the message. It turns out that this is the word, "pine".

After decrypting most of the message in this tedious manner, 25 digraph mappings can be derived in which one of the letters in the plaintext diagraph repeats in the encrypted diagraph. From those mappings, the key table can be derived using similar analysis as was presented above for the A R O V E sequence.

Warriors of the Rapture

To generalize the solution, consider a ladder with *N* rungs and let *f(N)* be the number of ways an applicant can ascend such a ladder. *f(1) = 1* since the only possible sequence for a ladder with 1 rung is: 1. *f(2) = 2* since with 2 rungs there are these sequences: 1,1; 2. And so on:

N	*f(N)*	Sequences
1	1	1
2	2	1,1; 2
3	3	1,1,1; 1,2; 2,1
4	5	1,1,1,1; 1,1,2; 1,2,1; 2,1,1; 2,2
5	8	1,1,1,1,1; 1,1,1,2; 1,1,2,1; 1,2,1,1; 2,1,1,1; 1,2,2; 2,1,2; 2,2,1

The sequence representing the ascent of a ladder with *N* rungs will either start with 1 or 2. In the case of 1, there are *f(N-1)* possible ways to ascend the remaining rungs. In the case of 2, there are *f(N-2)* possible ways to ascend the remaining rungs. Hence, the total number of ways to ascend the ladder with *N* rungs is the sum of *f(N-1)* and *f(N-2)*. To summarize:

f(1) = 1
f(2) = 2
f(N) = f(N-1) + f(N-2)

This recursive definition is consistent with definition of the Fibonacci function: *f(N) = fib(N)*. Here is a table of the first few values that will be useful below:

N	1	2	3	4	5	6	7	8	9	10	11
fib(N)	1	2	3	5	8	13	21	34	55	89	144

From the challenge problem, the judges inform the applicant on the first attempt and after the applicant takes two steps whether at least one of those initial two steps are incorrect.

There are 4 possible ways to start the sequence. Each way traverses a certain number of rungs:

Steps	Rungs
1,1	2
1,2	3
2,1	3
2,2	4

For the first way, if the applicant is told that neither of the first two steps are incorrect, then there are *fib(N-2)* possible sequences. The "*-2*" comes from the number of rungs already traversed. If either of the first two steps is incorrect, then in the worst case scenario, the applicant must try all 3 of the other possible starts. Each of them in turn has a cost of *fib(N-3)*, *fib(N-3)* and *fib(N-4)* respectively and the total cost is the sum of those costs. Another way to view this is *fib(N) - fib(N-2)* because there are *fib(N)* total sequences and *fib(N-2)* ways to start with 1,1. Note that:

fib(N-3) + fib(N-3) + fib(N-4) = fib(N-3) + fib(N-2) = fib(N-1) *fib(N) - fib(N-2) = fib(N-1) + fib(N-2) - fib(N-2) = fib(N-1)*

Repeating this idea with all the initial sequences yields these results:

Steps	Correct Start	Incorrect Start
1,1	*fib(N-2)*	*1 + fib(N) - fib(N-2)*
1,2	*fib(N-3)*	*1 + fib(N) - fib(N-3)*
2,1	*fib(N-3)*	*1 + fib(N) - fib(N-3)*
2,2	*fib(N-4)*	*1 + fib(N) - fib(N-4)*

The "1 +" comes from the initial incorrect attempt. The idea can be summarized as follows: Let *X* be number of rungs traversed in the initial 2 steps. If the first attempt contains the correct start, then it will have a cost of *fib(N-X)*. Otherwise, the cost is *1 + fib(N) - fib(N-X)*.

The table above can be converted to to:

Steps	Correct Start	Incorrect Start
1,1	*fib(N-2)*	*1 + fib(N-2) + fib(N-3)*
1,2	*fib(N-3)*	*1 + fib(N-2) + fib(N-2)*
2,1	*fib(N-3)*	*1 + fib(N-2) + fib(N-2)*
2,2	*fib(N-4)*	*1 + fib(N-2) + fib(N-3) + fib(N-3)*

In this form, it's easy to see that the incorrect start is always more costly than the correct start. It's also clear that the least expensive incorrect start is for the 1,1 sequence.

For an eight-rung ladder, the applicant should start with 1,1 and in the worst-case scenario the applicant will have to ascend the ladder *1 + fib(6) + fib(5) = 1 + 13 + 8 = 22* times. To get a sense of how cost effective this strategy is, here's the table for the eight-rung ladder:

Steps	Correct Start	Incorrect Start
1,1	13	22
1,2	8	27
2,1	8	27
2,2	5	30

Note that each row adds up to 35, which equals *1 + fib(8)*. This makes sense because the incorrect start column must take into account the initial attempt.

What Color is my Hat?

Before addressing the challenge problem, consider the general approach to this puzzle. All the possible solutions can be represented in a table like this:

	Hat Color	Shirt Color	Pants Color
Mr. Red	red, green, blue	red, green, blue	red, green, blue
Mr. Green	red, green, blue	red, green, blue	red, green, blue
Mr. Blue	red, green, blue	red, green, blue	red, green, blue

Each cell starts out with a set of all the possible colors. Since there are 3 colors, the initial set size for all the sets is 3. Next, the hints are introduced into the table. Problem 1 states that Mr. Green wears green pants and Mr. Red wears a red shirt. When this information is introduced, the size of two of the sets is reduced to 1:

	Hat Color	Shirt Color	Pants Color
Mr. Red	red, green, blue	red	red, green, blue
Mr. Green	red, green, blue	red, green, blue	green
Mr. Blue	red, green, blue	red, green, blue	red, green, blue

The puzzle provides the constraint that across any row and down any column, each color can only appear once. If the hints are sufficient to solve the puzzle, repeatedly applying this constraint will ultimately reduce all the sets to size 1. Apply the following analysis to each row:

1. For each set containing a single color, remove that color from the remaining sets in the row. This comes directly from the puzzle constraint.
2. Locate 2 matching sets containing exactly 2 colors. The remaining set in the row must contain only the remaining color.

Then, repeat that analysis to each column and then again to the rows and so on until none of the sets are further reduced.

Analyzing the rows reduces the sets as follows:

	Hat Color	Shirt Color	Pants Color
Mr. Red	~~red~~, green, blue	**red**	~~red~~, green, blue
Mr. Green	red, ~~green~~, blue	red, ~~green~~, blue	**green**
Mr. Blue	red, green, blue	red, green, blue	red, green, blue

Analyzing the columns further reduces the sets to this:

	Hat Color	Shirt Color	Pants Color
Mr. Red	green, blue	**red**	~~green~~, blue
Mr. Green	red, blue	~~red~~, blue	**green**
Mr. Blue	red, green, blue	~~red~~, green, blue	red, ~~green~~, blue

Again applying the analysis to the rows:

	Hat Color	Shirt Color	Pants Color
Mr. Red	green, ~~blue~~	red	**blue**
Mr. Green	red, ~~blue~~	**blue**	green
Mr. Blue	red, green, blue	green, blue	red, blue

And one last time to the columns:

	Hat Color	Shirt Color	Pants Color
Mr. Red	**green**	red	**blue**
Mr. Green	**red**	**blue**	green
Mr. Blue	~~red~~, ~~green~~, blue	green, ~~blue~~	red, ~~blue~~

Repeating any further fails to reduce any of the sets. Since all the sets were reduced to size 1, this problem was solvable with the provided hints.

Now consider problem 2, which provides 4 hints:

i. Mr. Green doesn't wear a red shirt.
ii. Mr. Green doesn't wear a blue hat.
iii. Mr. Red doesn't wear a red shirt.
iv. Mr. Red doesn't wear red pants.

Introducing them generates this table:

	Hat Color	Shirt Color	Pants Color
Mr. Red	red, green, blue	~~red~~, green, blue	~~red~~, green, blue
Mr. Green	red, green, ~~blue~~	~~red~~, green, blue	red, green, blue
Mr. Blue	red, green, blue	red, green, blue	red, green, blue

When the top row is analyzed, a pair of matching sets of size 2 is found: { green, blue }. Either the shirt is green and the pants are blue or vice versa. The hat must be red because neither the shirt nor the pants are red. The other two rows cannot be reduced on the first pass:

	Hat Color	Shirt Color	Pants Color
Mr. Red	red, ~~green~~, ~~blue~~	**green, blue**	**green, blue**
Mr. Green	red, green	green, blue	red, green, blue
Mr. Blue	red, green, blue	red, green, blue	red, green, blue

Next, the columns are analyzed:

	Hat Color	**Shirt Color**	**Pants Color**
Mr. Red	**red**	**green, blue**	green, blue
Mr. Green	~~red~~, green	**green, blue**	red, green, blue
Mr. Blue	~~red~~, green, blue	red, ~~green~~, ~~blue~~	red, green, blue

And so on until the analysis fails to reduce any of the sets:

	Hat Color	**Shirt Color**	**Pants Color**
Mr. Red	red	green, blue	green, blue
Mr. Green	**green**	~~green~~, blue	red, ~~green~~, blue
Mr. Blue	green, blue	**red**	~~red~~, green, blue

	Hat Color	**Shirt Color**	**Pants Color**
Mr. Red	red	green, ~~blue~~	**green, blue**
Mr. Green	**green**	**blue**	red, ~~blue~~
Mr. Blue	~~green~~, blue	red	**green, blue**

	Hat Color	**Shirt Color**	**Pants Color**
Mr. Red	red	**green**	~~green~~, blue
Mr. Green	green	blue	red
Mr. Blue	**blue**	red	green, ~~blue~~

Now, how many ways are there to dress the 3 people while maintaining the color constraint proposed by the puzzle? To answer that, consider this table:

	Hat Color	**Shirt Color**	**Pants Color**
Mr. Red	X	Y	Z
Mr. Green	?	?	?
Mr. Blue	?	?	?

X, Y and Z represent the distinct colors across the top row. There are 6 possible ways to assign these variables:

X	**Y**	**Z**
red	green	blue
red	blue	green
green	red	blue
green	blue	red
blue	red	green
blue	green	red

In the puzzle solution, X must appear in each row exactly once. For the second row, it cannot appear in the Hat Color column since it's already there in the first row. It can either be in the Shirt Color column or the Pants Color column. If it is in the Shirt Color column, then it must appear in the Pants Color column in the third row:

	Hat Color	Shirt Color	Pants Color
Mr. Red	X	Y	Z
Mr. Green	?	**X**	?
Mr. Blue	?	?	**X**

The remaining unknown shirt color must be Z and the remaining unknown pants color must be Y. Finally, the remaining hat colors can be deduced:

X-in-middle Table

	Hat Color	Shirt Color	Pants Color
Mr. Red	X	Y	Z
Mr. Green	Z	X	Y
Mr. Blue	Y	Z	X

If X were instead placed in the Pants Color column in the second row, then it must appear in the Shirt Color column in the third row. Again, the remaining cell values can be deduced:

Z-in-middle Table

	Hat Color	Shirt Color	Pants Color
Mr. Red	X	Y	Z
Mr. Green	Y	Z	X
Mr. Blue	Z	X	Y

After placing X, Y and Z across the first row, these two tables represent the only possible ways to fill the second and third rows. Since there are 6 ways to assign the variables, there are only 12 possible ways to dress the people.

Now, the hints in the challenge problem are the type of hints used in Problem 1. Each hint specifies the color of an article of clothing and who is wearing it. If one hint were given for each of the cells across the top row, such as:

i. Mr. Red wears a red hat.
ii. Mr. Red wears a green shirt.
iii. Mr. Red wears blue pants.

Then, the values of X, Y and Z are specified, but it is impossible to determine if the solution is of the form of the X-in-middle table or the Z-in-middle table. In fact, this is true if the 3 hints are provided across any row or down any column because X, Y and Z appear only once in those as well. So, there are puzzles with 3 non-redundant hints that are not solvable. What about 4 hints?

The table below combines the X-in-middle table with the Z-in-middle table.

Combined Table

	Hat Color	Shirt Color	Pants Color
Mr. Red	X/X	Y/Y	Z/Z
Mr. Green	Y/Z	Z/X	X/Y
Mr. Blue	Z/Y	X/Z	Y/X

Since there are only 3 colors, for 4 hints, at least 2 of the hints must specify clothing articles with a common color. Suppose a pair of common color hints both refer to cells that <u>may</u> contain X. There are 6 ways this can happen:

1. **X**/X, **X**/Y
2. **X**/X, **X**/Z
3. **X**/Y, **X**/Z
4. X/**X**, Z/**X**
5. X/**X**, Y/**X**
6. Z/**X**, Y/**X**

Note that each pair is either of the form { X/A, X/B } or { A/X, B/X } where A <u>never</u> equals B. The first 3 pairs only exist in the X-in-middle table and the last 3 pairs only exist in the Z-in-middle table. This means that a pair of common color hints that both refer to cells that may contain X actually specifies the value of X and determines which of the 2 tables the solution must conform to. The same analysis can be applied to Y and Z with an analogous result.

With the table type known, the 4 hints specify the values of 4 cells. Since each variable only occupies 3 cells, 4 hints must specify the values of at least 2 variables. Once the values of the 2 variables are known, the value of the third variable is the remaining color.

In summary, with only 3 hints, it is possible there is no solution; however, with 4 or more hints, the solution can always be determined.

Lying Socks

For the challenge problem, it is possible to determine the 3 properties using at most 8 yes-or-no questions. Here's the decision tree summarized as nested conditional statements:

```
Ask ABC if shoe
  Agree: Ask ABC about remainder
    Agree: [6]
    Disagree: Ask D about remainder
      3-1: [7]
      2-2: Ask E about remainder [8]
  Disagree: Ask D if shoe
    3-1: Identified 1 liar. Ask any 2 others about remainder
      Agree: [6]
      Disagree: Ask a truth-teller about remainder [7]
    2-2: Ask E if shoe. Ask E about remainder [6]
```

Begin by asking A, B and C if the object is a shoe (line 1). In a group of 3 people, at least 1 of them must be a truth-teller. If they are all asked the same question and they all provide the same answer, then all of them must have told the truth because the remaining 2 people agreed with the truth-teller. If they agree it is a shoe, then as described by the challenge problem, it must be large. If they agree that it is not a shoe, then it must be a black sock. In either case, if they all agree (line 2), then ask all 3 of them all about the remaining property. If they all agree again (line 3), then all the properties are now known and it only took 6 questions. If they disagree about the remaining property (line 4), then ask D about it. There are 2 possible outcomes. First, 3 people provided the same answer and 1 person gave a different answer (line 5). As discussed above, if a group 3 people agree, then that answer is valid; hence, the analysis is complete in 7 questions. The other possibility is that 2 people gave one answer and the other 2 gave the opposite answer (line 6). This is only possible if 2 of the 4 the people are occasional liars. So, E and F must be truth-tellers. Ask E about the remaining property to finish with 8 questions.

Returning to line 1, if there is no consensus, then ask D if the object is a shoe (line 7). There are 2 possible outcomes. First, 3 people provided the same answer and 1 person gave a different answer (line 8). The majority answer determines whether the object is a large shoe or a black sock. Also, since one of the 3 people that agreed is a truth-teller, the person that disagreed must be an occasional liar. With one occasional liar identified among the 6 people, ask 2 of the remaining 5 people about the last property. At least 1 of those 2 people must be a truth-teller because there are only 2 occasional liars in total. If those 2 people agree (line 9), then that answer is valid and it took 6 questions. If those 2 people disagree (line 10), then 1 of them is an occasional liar. Discounting them and the identified occasional liar, 3 people remain and they must be truth-tellers. Ask any of them about the remaining property to finish with 7 questions.

Finally, for line 11, A, B, C and D were asked if it is a shoe. Two of them provided one answer and the other two provided the opposite answer. This is only possible if 2 of those 4 people are occasional liars and hence, E and F must be truth-tellers. Ask E if the object is a shoe and then ask E about the remaining property to complete with 6 questions.

There are slight variations to this solution. For instance, instead of starting out by asking A, B and C if it is shoe, asking if the object is a sock would have sufficed just as well. On line 2, instead of asking A, B and C about the final property, any 3 people, such as D, E and F would have worked also.

Revisiting Rose's Message

The ballots are in one of two places. They are **22** miles south and two miles west of the entrance to the public library in Hood River. Find the largest pine and dig down **3** feet. If that doesn't work try **8** miles east of the ranger station on the old highway east of Hood River and go up twenty feet. Look for the juniper.