Криптографические алгоритмы и особенности их применения

Задание № 1.
Условие задачи
Исходный алфавит {A, B, C, D}.
Используется моноалфавитная система, в которой индивидуальные буквы зашифровываются так:

$$A \rightarrow BB,\ B \rightarrow AAB,\ C \rightarrow BAB,\ D \rightarrow A$$

Например, слово ABDA зашифровывается как BBAABABB. Докажите, что расшифрование всегда однозначно.
Покажите, что оно не будет однозначным, если буквы зашифровывать так:

$$A \rightarrow AB,\ B \rightarrow BA,\ C \rightarrow A,\ D \rightarrow C$$

Решение:

Достаточное условие однозначной декодируемости:
Сообщение декодируется однозначно, если для используемого кода выполняется прямое или обратное условие Фано

Условие Фано. *Никакое кодовое слово не совпадает с началом другого кодового слова. (Если в код входит слово a, то для любой непустой строки b слова ab в коде не существует.)*

Как мы можем увидеть для первой моноалфавитной системы выполняется обратное условие Фано:
Ни одна кодовая буква не является окончанием другой кодовой буквы из алфавита и, мы можем однозначно расшифровывать любое сообщение с конца, так как для любого набора символов будет возможен только один вариант расшифрования из алфавита

Для второго алфавита однако условие Фано не выполняется ни прямо, ни обратно. Код буквы C совпадает с началом и окончанием кодов A и B соответственно. Таким образом при расшифровке сообщений с подстроками начинающимися/оканчивающимися с A будет возможно более одного способа прочтения

Задание № 3.
При передаче сообщений используется некоторый шифр. Известно, что каждому из трёх шифрованных текстов:

ЙМЫВОТСЬЛКЪГВЦАЯЯ
УКМАПОЧСРКЩВЗАХ
ШМФЭОГЧСЙЪКФЬВЫЕАКК

соответствовало исходное сообщение **МОСКВА**.
Дешифруйте три текста:
ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯРЯ
ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЬЕП
РТПАИОМВСВТИЕОБПРОЕННИГЬКЕЕАМТАЛВТДЬСОУМЧШСЕОНШЬИАЯК

при условии, что двум из них соответствует одно и то же сообщение. Сообщениями являются крылатые фразы.

Решение:
Посмотрев на шифры соответствующие слову МОСКВА, можно заметить и предположить, что слова шифруются путем вставки между буквами 1 или 2 других букв (в скобках указано сколько цепочка показывающая сколько букв было вставлено).
Я не нашла других закономерностей в том как вставляются эти буквы и просто перебирала варианты до получения осмысленного результата. Первое и третье сообщение одна крылатая фраза за исключением,может быть, написания.

1) **ЙМЫВОТСЬЛКЪГВЦАЯЯ** *(1212212)*
2) **УКМАПОЧСРКЩВЗАХ** *(2211111)*
3) **ШМФЭОГЧСЙЪКФЬВЫЕАКК** *(1222222)*

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯРЯ
11211211211212122112
ПОВТОРЕНИЕМАТЬУЧЕНИЯ

ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЬЕП
12111212122212
СМОТРИВКОРЕНЬ

РТПАИОМВСВТИЕОБПРОЕННИГЬКЕЕАМТАЛВТДЬСОУМЧШСЕОНШЬИАЯК
22122211212121212121
ПОВТОРЕНЬЕМАТЬУЧЕНЬЯ