TEACH 13: PROBLEM SET

Exercises

1. Which is inherently stronger: block or stream ciphers? Explain your rational.

Block ciphers are stronger because they allow for better performance and because they allow for more complex algorithms to be used.

2. Name a situation when Steganography would be better choice than cryptography.

Steganography would be better than cryptography in the case of a husband sending messages to his wife’s friends informing them of a surprise party for her. If she learns of the messages, she likely doesn’t need to read them to guess what they are about.

Problems

3. Which is more resistant to Golden Bug attacks: transposition or substitution ciphers? Explain your rational.

Substitution ciphers would likely be more resistant to Golden Bug attacks because substitution changes the letters that are being used so it is harder to determine what the text is based on the frequency of the letters. Transposition keeps the same letters and just changes their order.

4. Is the Golden Bug ratio the same for all languages? Explain your rational.

The Golden Bug ratio is not the same for all languages because different languages can have different letters and all likely have different frequency of letters.

5. How many guesses will it take to crack a Caesar Cipher message of Cyrillic text? Hint: how many characters are there in the Cyrillic alphabet?

The maximum number of guesses depends on if numbers are included or only letters. If there are only letters, then the answer is 33 (the number of letters in Cyrillic) otherwise it would be 43.

6. How large is the key-size (in bits) of a single Chinese character? Hint: How many characters are there in the Chinese alphabet?

There are conflicting reports on how many Chinese characters there are. Most dictionaries include about 5000 and in that case the key-size would be 13.

Challenges

7. How can cracking efforts be frustrated by a carefully chosen plain-text message? Hint: What plain-text message would be more difficult to crack?

It is very important to carefully choose the plain-text message. Golden bug is a common plaintext attack. Where the message can be decrypted by the analyzing the frequency of a letter. For example, the most dominant letter in English is the letter e with an average of 12.7 percent. So, if the attacker finds the most frequent letter, it will be very easy to crack the message.   
 The chosen amount and nature of plain-text also makes cracking of plain text more difficult. If we have a different type of character let's say text and numbers and the algorithm ciphers differently for those two different types of character then it gets hard to guess total combination.

8. Crack the following message encrypted with Caesar Cipher:

"MANYYEARSAGOICONTRACTEDANINTIMACYWITHAMRWILLIAM(LEGRANDHEWASOFANANCIENTHUGUENOTFAMILYANDHADONCE(BEENWEALTHYBUTASERIESOFMISFORTUNESHADREDUCEDHIM(TOWANTTOAVOIDTHEMORTIFICATIONCONSEQUENTUPONHISD(ISASTERSHELEFTNEWORLEANSTHECITYOFHISFOREFATHERS(ANDTOOKUPHISRESIDENCEATSULLIVANSISLANDNEARCHARL(ESTONSOUTHCAROLINATHISISLANDISAVERYSINGULARONEI(TCONSISTSOFLITTLEELSETHANTHESEASANDANDISABOUTTH(REEMILESLONGITSBREADTHATNOPOINTEXCEEDSAQUARTERO(FAMILEITISSEPARATEDFROMTHEMAINLANDBYASCARCELYPE(RCEPTIBLECREEKOOZINGITSWAYTHROUGHAWILDERNESSOFR(EEDSANDSLIMEAFAVORITERESORTOFTHEMARSHHENTHEVEGE(TATIONASMIGHTBESUPPOSEDISSCANTORATLEASTDWARFISH(NOTREESOFANYMAGNITUDEARETOBESEENNEARTHEWESTERNE(XTREMITYWHEREFORTMOULTRIESTANDSANDWHEREARESOMEM(ISERABLEFRAMEBUILDINGSTENANTEDDURINGSUMMERBYTHE(FUGITIVESFROMCHARLESTONDUSTANDFEVERMAYBEFOUNDIN(DEEDTHEBRISTLYPALMETTOBUTTHEWHOLEISLANDWITHTHEE(XCEPTIONOFTHISWESTERNPOINTANDALINEOFHARDWHITEBE(ACHONTHESEACOASTISCOVEREDWITHADENSEUNDERGROWTHO(FTHESWEETMYRTLESOMUCHPRIZEDBYTHEHORTICULTURISTS(OFENGLANDTHESHRUBHEREOFTENATTAINSTHEHEIGHTOFFIF(TEENORTWENTYFEETANDFORMSANALMOSTIMPENETRABLECOP(PICEBURTHENINGTHEAIRWITHITSFRAGRANCE"

Q5

9. If I use a 1-bit hash, how much change in the message can be detected? In other words, how much or little can I change the message without the recipient noticing? Hint: a 1-bit hash works much like a check-sum. You might need to do some research to see how a check-sum works.

I think, it is 50%. One can change 50% until it can be detected.

10. If the message is a 32-bit number, how large must the hash be to be absolutely secure? In other words, how large must the hash be so that any change in the message will be detected by the recipient? Hint: to be "absolutely secure," there must be exactly one message that maps to a given hash.

5 bits

11. If the message is a 8 letter ASCII password, how large in bits must the hash be to be absolutely secure?

11 bits

12. Consider a message consisting of several pages of text. I am going to use a single 16-bit number as my hash value. What is the probability that a random change to the document will result in the hash still matching the message?

1/65,536