Eamonn Keogh - C16757629

Advanced Security 1 - Lab 2

Question 1

After some experimentation and randomly trying out different key values I discovered that a **key value of three** resulted in a legible message in the english language. The decrypted message read as follows:

ONE VARIATION TO THE STANDARD CAESAR CIPHER IS WHEN THE ALPHABET IS "KEYED" BY USING A WORD. IN THE TRADITIONAL VARIETY, ONE COULD WRITE THE ALPHABET ON TWO STRIPS AND JUST MATCH UP THE STRIPS AFTER SLIDING THE BOTTOM STRIP TO THE LEFT OR RIGHT. TO ENCODE, YOU WOULD FIND A LETTER IN THE TOP ROW AND SUBSTITUTE IT FOR THE LETTER IN THE BOTTOM ROW. FOR A KEYED VERSION, ONE WOULD NOT USE A STANDARD ALPHABET, BUT WOULD FIRST WRITE A WORD (OMITTING DUPLICATED LETTERS) AND THEN WRITE THE REMAINING LETTERS OF THE ALPHABET. FOR THE EXAMPLE BELOW, I USED A KEY OF "RUMKIN.COM" AND YOU WILL SEE THAT THE PERIOD IS REMOVED BECAUSE IT IS NOT A LETTER. YOU WILL ALSO NOTICE THE SECOND "M" IS NOT INCLUDED BECAUSE THERE WAS AN M ALREADY AND YOU CAN'T HAVE DUPLICATES.

Question 2

Similar to the method used above I randomly selected various keys until I discovered that a **key value of 17** gave a legible result in the english language. The decrypted message read as follows:

ONE VARIATION TO THE STANDARD CAESAR CIPHER IS WHEN THE ALPHABET IS "KEYED" BY USING A WORD. IN THE TRADITIONAL VARIETY, ONE COULD WRITE THE ALPHABET ON TWO STRIPS AND JUST MATCH UP THE STRIPS AFTER SLIDING THE BOTTOM STRIP TO THE LEFT OR RIGHT. TO ENCODE, YOU WOULD FIND A LETTER IN THE TOP ROW AND SUBSTITUTE IT FOR THE LETTER IN THE BOTTOM ROW. FOR A KEYED VERSION, ONE WOULD NOT USE A STANDARD ALPHABET, BUT WOULD FIRST WRITE A WORD (OMITTING DUPLICATED LETTERS) AND THEN WRITE THE REMAINING LETTERS OF THE ALPHABET. FOR THE EXAMPLE BELOW, I USED A KEY OF "RUMKIN.COM" AND YOU WILL SEE THAT THE PERIOD IS REMOVED BECAUSE IT IS NOT A LETTER. YOU WILL ALSO NOTICE THE SECOND "M" IS NOT INCLUDED BECAUSE THERE WAS AN M ALREADY AND YOU CAN'T HAVE DUPLICATES.

Question 3

After decrypting the message it revealed the following plaintext:

NIST IS ABOUT TO ANNOUNCE THE NEW HASH ALGORITHM THAT WILL BECOME SHA-3. THIS IS THE RESULT OF A SIX-YEAR COMPETITION, AND MY OWN SKEIN IS ONE OF THE FIVE REMAINING FINALISTS (OUT OF AN INITIAL 64). IT'S PROBABLY TOO LATE FOR ME TO AFFECT THE FINAL DECISION, BUT I AM HOPING FOR "NO AWARD." IT'S NOT THAT THE NEW HASH FUNCTIONS AREN'T ANY GOOD, IT'S THAT WE DON'T REALLY NEED ONE. WHEN WE STARTED THIS PROCESS BACK IN 2006, IT LOOKED AS IF WE WOULD BE NEEDING A NEW HASH FUNCTION SOON. THE SHA FAMILY (WHICH IS REALLY PART OF THE MD4 AND MD5 FAMILY), WAS UNDER INCREASING PRESSURE FROM NEW TYPES OF CRYPTANALYSIS. WE DIDN'T KNOW HOW LONG THE VARIOUS SHA-2 VARIANTS WOULD REMAIN SECURE. BUT IT'S 2012, AND SHA-512 IS STILL LOOKING GOOD.
EVEN WORSE, NONE OF THE SHA-3 CANDIDATES IS SIGNIFICANTLY BETTER. SOME ARE FASTER, BUT NOT ORDERS OF MAGNITUDE FASTER. SOME ARE SMALLER IN HARDWARE, BUT NOT ORDERS OF MAGNITUDE SMALLER. WHEN SHA-3 IS ANNOUNCED, I'M GOING TO RECOMMEND THAT, UNLESS THE IMPROVEMENTS ARE CRITICAL TO THEIR APPLICATION, PEOPLE STICK WITH THE TRIED AND TRUE SHA-512. AT LEAST FOR A WHILE. I DON'T THINK NIST IS GOING TO ANNOUNCE "NO AWARD"; I THINK IT'S GOING TO PICK ONE. AND OF THE FIVE REMAINING, I DON'T REALLY HAVE A FAVORITE. OF COURSE I WANT SKEIN TO WIN, BUT THAT'S OUT OF PERSONAL PRIDE, NOT FOR SOME OBJECTIVE REASON. AND WHILE I LIKE SOME MORE THAN OTHERS, I THINK ANY WOULD BE OKAY. WELL, MAYBE THERE'S ONE REASON NIST SHOULD CHOOSE SKEIN. SKEIN ISN'T JUST A HASH FUNCTION, IT'S THE LARGE-BLOCK CIPHER THREEFISH AND A MECHANISM TO TURN IT INTO A HASH FUNCTION. I THINK THE WORLD ACTUALLY NEEDS A LARGE-BLOCK CIPHER, AND IF NIST CHOOSES SKEIN, WE'LL GET ONE.

Question 4

I had never seen this type of ciphertext before so I had to go digging around on the internet, I learned that its technically not a ciphertext but an encoding scheme that represents binary data in an ASCII string. This encoding scheme is known as **Base64 cipher**.After decrypting the text string with an online tool the following message was shown:

On Thursday Google announced that the next version of Android will have encryption enabled by default, protecting user data from anyone who lacks password access. It's a feature lauded by privacy advocates, and matches Apple's new iPhone policy. But Google's new policy isn't very helpful if you own an Android phone that won't be updated to Android L

for a while (if ever). But let's not get too bent out of shape. We're here to share how you can encrypt your Android devices running the Jelly Bean and Kit Kat systems. That's right: Privacy features are already built in. You just need to turn them on.

Question 5

From reading a few lines of the text I could see that the characters 0, 1, 2, 3, 4, 5, 6, 7, 8 ,9, a, b, c, d, e, f where present, meaning that its highly likely that the message was encoded into **hexadecimal** values as there were no other characters present. Although I didn't read the entire ciphertext, just skimmed it. To confirm my suspicion I ran the text through a hexadecimal to text decoder online. The message displayed as follows:

On Thursday Google announced that the next version of Android will have encryption enabled by default, protecting user data from anyone who lacks password access. It's a feature lauded by privacy advocates, and matches Apple's new iPhone policy. But Google's new policy isn't very helpful if you own an Android phone that won't be updated to Android L for a while (if ever). But let's not get too bent out of shape. We're here to share how you can encrypt your Android devices running the Jelly Bean and Kit Kat systems. That's right: Privacy features are already built in. You just need to turn them on.

Question 6

After trying different shift key values of 1, 2 and 3, with 3 resulting in 'Joseph' being discovered on the end of the 2nd line of text. However, the remainder of the text being gibberish to me, I decided to experiment with translating the message into various languages. The decrypted message without translation was as follows:

CHAMA Cha Mapinduzi pamoja na vijana wake kupitia umoja wao wa UVCCM, kimemshukia aliyekuwa Mwenyekiti wa Tume ya Mabadiliko ya Katiba, Jaji Joseph Warioba, kikimtaka aache kujidanganya, kwani suala la Katiba mpya haliwezi kuwa ajenda ya uchaguzi mkuu, mwakani. Kwa upande wa UVCCM, imemtaka Jaji Warioba, aache mara moja kutumia dhamana aliyokuwa amepewa ya kuwa Mwenyekiti wa Tume ya Mabadiliko ya Katiba, kwani muda wake umeishamalizika kisheria. Kauli hizo zilitolewa kwa nyakati tofauti na viongozi wa chama hicho, ikiwa ni siku chache tangu Jaji Warioba atoe maoni yake kuhusiana na Rasimu iliyopendekezwa na Bunge Maalum la Katiba, ambapo alikosoa kutokana na kuachwa kwa baadhi ya maoni ya wananchi. Aidha, ameendelea kusisitiza kuwa, atakuwa Rais wa Watanzania, bila kujali dini, kabila au vyama, hivyo maendeleo ya serikali yake hayatabagua. Akizungumza jana mjini hapa kwenye mkutano wa kampeni uliohudhuriwa na maelfu ya watu ambao alikiri kuwa ni mkubwa ambao hajawahi kuuona, amewahakikishia kuwa ataiendesha nchi kwa ustaarabu na si kwa udikteta kama ambavyo baadhi ya watu wamekuwa wakidai. Hata baada ya kuchaguliwa, mimi sitabadilika, nitabaki kuwa mtoto wenu yule yule John Magufuli, alisema na kuongeza; Nitaiendesha nchi kwa ustaarabu, sitaiendesha nchi kwa udikteta pamekuwa na watu wanazungumza, kwa sababu nazungumza ukweli na ukweli utabaki ukweli kweli. Watu wanabaki kutishiana. Nyie wana Chato waelezeni ukweli kwamba nilipokuwa waziri nilikuwa nachunga ng'ombe, nilikuwa nakamua maziwa.

By inserting the above text into Google translate (which figured out it was swahilli) the message then translated to:

The Revolutionary Party and its youth through their UVCCM coalition, descended the Chairman of the Constitutional Commission, Justice Joseph Warioba, wanting him to stop deceiving himself, since the subject of the new Constitution cannot be the general election agenda, next year. On behalf of the UVCCM, it has called for Judge Warioba, cease immediately to use the guarantee he had been given as Chairman of the Commission Constitutional change, as it is legally expired. Such statements were issued at different times by party leaders, if only a few days since Judge Warioba should comment on the Draft proposed by the Special Assembly of the Constitution, in which he was criticized for the abandonment of some public opinion. He further emphasized that he will be the President of Tanzanians, regardless of religion, tribe or parties, so the development of its government will not discriminate. Speaking of yesterday in town here at a campaign rally attended by the thousands of people he admitted being the greatest he has never seen, he has assured them that he will run the country for civilization and not by dictatorship as some people have been claiming. Even after being elected, I will not change, I will remain the same child John Magufuli, said and added; I will run the country civilized, I will not run it the country by dictatorship there have been people talking, because I speak the truth with truth will remain true truth. People remain threatening each other. You guys have Chato explain the fact that as a minister I was herding cattle, I was picking milk.