Advanced Security Lab 2:

Cormac Smith C17723185

Q1.

Key Used: 3

ONE VARIATION TO THE STANDARD CAESAR CIPHER IS WHEN THE ALPHABET IS "KEYED" BY USING A WORD. IN THETRADITIONAL VARIETY, ONE COULD WRITE THE ALPHABET ONTWO STRIPS AND JUST MATCH UP THE STRIPS AFTER SLIDINGTHE BOTTOM STRIP TO THE LEFT OR RIGHT. TO ENCODE, YOUWOULD FIND A LETTER IN THE TOP ROW AND SUBSTITUTE ITFOR THE LETTER IN THE BOTTOM ROW. FOR A KEYED VERSION, ONE WOULD NOT USE A STANDARD ALPHABET, BUT WOULD FIRSTWRITE A WORD (OMITTING DUPLICATED LETTERS) AND THENWRITE THE REMAINING LETTERS OF THE ALPHABET. FOR THEEXAMPLE BELOW, I USED A KEY OF "RUMKIN.COM" AND YOU WILL SEETHAT THE PERIOD IS REMOVED BECAUSE IT IS NOT A LETTER.YOU WILL ALSO NOTICE THE SECOND "M" IS NOT INCLUDEDBECAUSE THERE WAS AN M ALREADY AND YOU CANT HAVEDUPLICATES.

Q2.

Key Used: 17

ONE VARIATION TO THE STANDARD CAESAR CIPHER IS WHEN THEALPHABET IS "KEYED" BY USING A WORD. IN THE TRADITIONALVARIETY, ONE COULD WRITE THE ALPHABET ON TWO STRIPS AND JUSTMATCH UP THE STRIPS AFTER SLIDING THE BOTTOM STRIP TO THELEFT OR RIGHT. TO ENCODE, YOU WOULD FIND A LETTER IN THE TOPROW AND SUBSTITUTE IT FOR THE LETTER IN THE BOTTOM ROW. FOR AKEYED VERSION, ONE WOULD NOT USE A STANDARD ALPHABET, BUTWOULD FIRST WRITE A WORD (OMITTING DUPLICATED LETTERS) ANDTHEN WRITE THE REMAINING LETTERS OF THE ALPHABET. FOR THEEXAMPLE BELOW, I USED A KEY OF "RUMKIN.COM" AND YOU WILL SEETHAT THE PERIOD IS REMOVED BECAUSE IT IS NOT A LETTER. YOUWILL ALSO NOTICE THE SECOND "M" IS NOT INCLUDED BECAUSE THEREWAS AN M ALREADY AND YOU CANT HAVE DUPLICATES.

Q3.

NIST IS ABOUT TO ANNOUNCE THE NEW HASH ALGORITHM THAT WILLBECOME SHA-3. THIS IS THE RESULT OF A SIX-YEAR COMPETITION, ANDMY OWN SKEIN IS ONE OF THE FIVE REMAINING FINALISTS (OUT OFAN INITIAL 64). IT'S PROBABLY TOO LATE FOR ME TO AFFECT THE FINALDECISION, BUT I AM HOPING FOR 'NO AWARD.' IT'S NOT THAT THE NEWHASH FUNCTIONS AREN'T ANY GOOD, IT'S THAT WE DON'T REALLY NEEDONE. WHEN WE STARTED THIS PROCESS BACK IN 2006, IT LOOKED AS IFWE WOULD BE NEEDING A NEW HASH FUNCTION SOON. THE SHAFAMILY (WHICH IS REALLY PART OF THE MD4 AND MD5 FAMILY), WASUNDER INCREASING PRESSURE FROM NEW TYPES OFCRYPTANALYSIS. WE DIDN'T KNOW HOW LONG THE VARIOUS SHA-2VARIANTS WOULD REMAIN SECURE.

BUT IT'S 2012, AND SHA-512 IS STILLLOOKING GOOD.EVEN WORSE, NONE OF THE SHA-3 CANDIDATES IS SIGNIFICANTLYBETTER. SOME ARE FASTER, BUT NOT ORDERS OF MAGNITUDE FASTER.SOME ARE SMALLER IN HARDWARE, BUT NOT ORDERS OF MAGNITUDESMALLER. WHEN SHA-3 IS ANNOUNCED, I'M GOING TO RECOMMENDTHAT, UNLESS THE IMPROVEMENTS ARE CRITICAL TO THEIRAPPLICATION, 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 FIVEREMAINING, I DON'T REALLY HAVE A FAVORITE. OF COURSE I WANTSKEIN TO WIN, BUT THAT'S OUT OF PERSONAL PRIDE, NOT FOR SOMEOBJECTIVE REASON. AND WHILE I LIKE SOME MORE THAN OTHERS, ITHINK ANY WOULD BE OKAY. WELL, MAYBE THERE'S ONE REASON NISTSHOULD CHOOSE SKEIN. SKEIN ISN'T JUST A HASH FUNCTION, IT'STHE LARGE-BLOCK CIPHER THREEFISH AND A MECHANISM TO TURN ITINTO A HASH FUNCTION. I THINK THE WORLD ACTUALLY NEEDS ALARGE-BLOCK CIPHER, AND IF NIST CHOOSES SKEIN, WE'LL GET ONE.

Q4.

Decoded using base64: <https://www.base64decode.org>

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.

Q5.

Decoded using Hex String: <http://string-functions.com/hex-string.aspx>

On Thursday Google announced that the next version of Android will have encryption enabled by default, protecting user data from a??yone who lacks password access. It's a feature lauded by privacy advocates, and matche?? Apple's new iPhone policy. But Google's ne?? policy isn't very helpful if you own an An??roid 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 h?ow you can encrypt your Android devices runn?ing the Jelly Bean and Kit Kat systems. Tha??'s right: Privacy features are already bui??t in. You just need to turn them on. ?

Q6.

Key: 3

Language is Swahili

CHAMA CHA MAPINDUZI PAMOJA NA VIJANA WAKE KUPITIA UMOJA WAO WA UVCCM,KIMEMSHUKIA ALIYEKUWA MWENYEKITI WA TUME YA MABADILIKO YA KATIBA, JAJI JOSEPHWARIOBA, KIKIMTAKA AACHE KUJIDANGANYA, KWANI SUALA LA KATIBA MPYA HALIWEZI KUWAAJENDA YA UCHAGUZI MKUU, MWAKANI. KWA UPANDE WA UVCCM, IMEMTAKA JAJI WARIOBA,AACHE MARA MOJA KUTUMIA DHAMANA ALIYOKUWA AMEPEWA YA KUWA MWENYEKITI WA TUME YAMABADILIKO YA KATIBA, KWANI MUDA WAKE UMEISHAMALIZIKA KISHERIA. KAULI HIZOZILITOLEWA KWA NYAKATI TOFAUTI NA VIONGOZI WA CHAMA HICHO, IKIWA NI SIKU CHACHE TANGUJAJI WARIOBA ATOE MAONI YAKE KUHUSIANA NA RASIMU ILIYOPENDEKEZWA NA BUNGE MAALUMLA 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 JANAMJINI HAPA KWENYE MKUTANO WA KAMPENI ULIOHUDHURIWA NA MAELFU YA WATU AMBAO ALIKIRIKUWA NI MKUBWA AMBAO HAJAWAHI KUUONA, AMEWAHAKIKISHIA KUWA ATAIENDESHA NCHI KWAUSTAARABU NA SI KWA UDIKTETA KAMA AMBAVYO BAADHI YA WATU WAMEKUWA WAKIDAI.