Advanced Security – Lab 2 Tim Browning - C14519547

Q1)

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.

Q2)

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.

Key = 9

Q3)

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.

Q4)

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.

Base64

Q5)

Q6)

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.

Language = Swahili