Ryan Young

CSE 3400

1/24/20

Homework 1

1.) *Modular arithmetic is an important number theory concept that appears in cryptography frequently. The following exercises are a review of the concept. If you are unfamiliar with modular arithmetic there are a number of good resources online to help to familiarize oneself (the Wikipedia article seems decent). Try to do a,b,c in your head; d,e may require pencil and paper. I am entirely aware that you could sim-ply use Wolfram Alpha or a Python shell to solve these, but I recommend not to, as these resources will not be available during an exam, and this does nothing to improve understanding.*
(a) (23 + 18) mod 17
(b)−7 mod 11
(c) 2^{128} mod 2^{64}
(d) (2^6 * 3^7) mod 13

a.) 23 + 18 = 41 mod 17 = 41/17 = 2 with a remainder of 7 so the answer is 7
b.) -7 / 11 = 0 remainder 4 so the answer is 4
c.) 2^{128} divided by 2^{64} is 2^{64} and the remainder is 0 so the answer is 0
d.) 2^6 * 3^7 is 64 * 2187 = 139968 / 13 = remainder of 10

2.) *Write the formulas for encryption and decryption of the ROT13 cipher. Write the formulas for the decryption of the Caesar and Az-By ciphers.*

The formula for encryption of the ROT 13 cipher is the same as the formula for the decryption of the ROT 13 cipher is given as E/D(c/p) = c/p + 13 (mod 26).
The formula for encryption of the Caesar Cipher is given by c = E(p) = p + 3 (mod 26) while the formula for decryption of the Caesar Cipher is given by p = D(c) = c-3 (mod 26).

3.) *(CPA > KPA > CTO). Explain (informally) why every cryptosystem vulnerable to CTO attack, is also vulnerable to KPA, and every cryptosystem vulnerable to KPA, is also vulnerable to CPA.*

Every system vulnerable to a CTO attack is also vulnerable to KPA and CPA attacks. This can be explained because CTO attacks work by using the frequencies of the English language to break the cipher. And while this may work on a weak system it will not work on higher security systems. KPA and CPA attacks work by either guessing which plaintext message the victim will send and then comparing it will the ciphertext or by having the pair already. Either way the KPA and CPA allows the attacker to have a full decryption of any message sent. Therefore, these attacks will work on a weaker system, but the weaker attack will not work on the stronger system. A KPA vulnerable system will be vulnerable to a CPA because the attacker was able to get the victim to send a plaintext message they want. This makes it easier to fully decrypt the rest of the messages and the attack stronger.

4.) *Suppose for some cryptosystem the key space is 256-bits. Suppose it takes a microsecond (1×10−6s), to perform a decryption of a given ciphertext. How long, in years, would it take to decrypt the ciphertext using every key in the key space.*

Given that the key space is 256 bits there are 2^{256} options for possible keys. If It takes a microsecond to perform decryption of a given cyphertext we would have 2^{256} Key * $\frac{1*10^{-6}s}{1\ key}$. This simplifies to $1.1579209*10^{77}$ * $\frac{1*10^{-6}s}{1\ key}$ = $1.1579209*10^{71}$ seconds. Converting this to minutes we divide by 60, converting this to hours we divide by 60, converting to days we divide by 24, and then converting to years we divide by 365. This results in an answer of $3.6717431*10^{63}$ years.

5.) *Describe an efficient table look-up attack for a mono-alphabetic substitution cipher. What pre-defined plaintext message would you use? How many table entries would be required? Hint: Look at section 2.1.3 in the notes.*

An efficient table look-up attack for a mono-alphabetic substation cipher would be one that compares the most commonly used letters in the English alphabet with the most commonly used letters in the cipher text. This would be a letter frequency attack (we are assuming the message is in plain English). I would use a common word such as “the” or “Hello” so that once the relationship is obvious between the ciphertext and plaintext I could use that to decode the rest. There would need to be $O(2^L)$ where L is the length of the message in this case because there is no key in a mono-alphabetic substation cipher.

6.) *Define the (stateful) encryption and decryption functions< E, D >for the One Time Pad (OTP) cipher. Note that below you should just fill in the answer after the. . .;I is taken to be an index for a particular bit.*

$E_k(m)$ =c where c[i] = k $\oplus$ m[i]
$D_k(c)$ =m where m[i] = k $\oplus$ c[i]