COMP90043 Cryptography and Security

Semester 2, 2021, Workshop Week 3 Solutions

Part A

1. What is a cipher? What does it do? And, in general, how does it go about doing this?
2. What is a block cipher and a stream cipher?

   A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

   A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.

3. What is a one-time pad? Discuss the practical applicability of the scheme in security?

   A one-time pad is a cryptographic scheme which uses a random key of equal length to the plain text to both encrypt and decrypt the message. While one-time padding offers complete security and is unbreakable, practical applicability is limited due to:

   - The requirement for a large quantity of random keys, in which the guarantee of true randomness of each character within the key is a significant task.
   - Key distribution is a major problem as each message has an associated key of equal length which needs to be known to the sender and receiver.

4. a. What is a symmetric cipher? What are the essential components of a symmetric cipher?

   A symmetric cipher is an enciphering primitive which uses the same cryptographic key to encrypt and decrypt the plaintext, known as the Secret Key which must only share with the intended receiver. There are five essential components of a symmetric cipher:

   - Plaintext – The original intelligible message or data.
   - Encryption Algorithm – An algorithm which performs various substitutions and transformations on the plaintext.
   - Secret Key – Is an input required for the encryption algorithm and is independent of the plaintext and the algorithm
   - Ciphertext – This is the scrambled message of the plaintext produced by the encryption algorithm as an output.
   - Decryption Algorithm – An algorithm which allows for the receiver to obtain the plaintext back from the ciphertext. For a symmetric cipher, the decryption algorithm is normally the encryption algorithm run in reverse.

   b. What is an asymmetric cipher? How does it different from a symmetric cipher? Cite at least two differences.

   An asymmetric cipher is an enciphering primitive which uses two different cryptographic keys as part of the enciphering process. One key which is used for encryption known as the Public Key which is shared to all senders; and another which is used for decryption known as the Private key which is kept secret by the receiver. Some differences:

   - Symmetric ciphers use only one cryptographic key whereas asymmetric ciphers use two.
   - Symmetric ciphers normally use one algorithm which runs forward for encryption and backwards for decryption. Asymmetric ciphers normally have two different algorithms, one for encryption and another for decryption.

- Symmetric ciphers are normally much faster than asymmetric ciphers.
- Symmetric ciphers are prone to the key sharing problem, asymmetric ciphers were introduced to resolve the key sharing problem.
- Symmetric ciphers are secure with smaller key sizes as the keys are always kept secret. Asymmetric ciphers need much larger key sizes as the public key is always available and can be reverse engineered to obtain the private key.

5. Let's consider cryptographic keys.
   a. What is it and why do we need one?

      A cryptographic key is a unique input to an encryption and decryption algorithm which acts as a seed allowing the algorithm to scramble the plaintext or to obtain the plaintext from the ciphertext. A cryptographic key is needed so as to facilitate the working for the enciphering primitive. For asymmetric ciphers the two keys are derived as two parts of a whole thereby together allowing for the encryption and decryption of the message. For symmetric ciphers the secret key acts as a offset seed which allows the algorithm to make consistent substitutions and transformations on the same message.

   b. List some of the different types of cryptographic keys used in practice.

      Symmetric ciphers use a Secret Key

      Asymmetric ciphers use a Public Key and a Private Key

   c. What are some of the security requirements for storing keys? How is this different when considering both symmetric ciphers and asymmetric ciphers?

      Symmetric ciphers are more prone to key storage requirements in contrast to asymmetric ciphers. As the secret key is the same for both encryption and decryption, symmetric ciphers face the key sharing problem; re how to transfer the secret key from the sender to the receiver without anyone intercepting this transmission. This problem was especially difficult when the sender and receiver were not in the same place at the same time. A good analogy is to imagine a box which is locked by user A and the locked box is then sent to User B. But the key to the box is now sealed in an envelope and mailed to User B. How can user B guarantee that no one intercepted this mail, opened the envelope, copied the key, and then resealed the key in another envelope and mailed it to User B?

      Asymmetric ciphers require the receiver to only keep his private key secret. In order to allow multiple senders to send messages he can broadcast this public key for anyone to obtain. As both the keys form a pair, and are used by different algorithms, an adversary needs to either obtain both keys or spend significant time reverse engineering the public key in order to obtain the private key to compromise the cipher.

      A widely used technique on the internet these days is to use a conjunction of both ciphers. Wherein a server sends a signed public key to a client. The client can then negotiate and generate a secret key and encrypt it using the server's public key and send it back to the server. The server then uses its private key to decrypt the message to obtain the shared key and then both parties can use the shared key to encrypt and decrypt further communications.

Part B

(1) Solve the following problems using Extended Euclid's algorithm using first principles. Make sure that you understand the process.

(a) $3^{-1}\ mod\ 7 =$ *5*

(b) $5^{-1}\ mod\ 13 =$ *8*

(c) $1473^{-1}\ mod\ 1562 =$ *351*

(d) $73^{-1}\ mod\ 127 =$ *87*

$7 = 3 \times 2 + 1$ $1 = 7 - 3 \times 2$ This shows the inverse is -2 (or 5 which is $-2\ mod\ 7$)	$13 = 5 \times 2 + 3$ $5 = 3 \times 1 + 2$ $3 = 2 \times 1 + 1$ $1 = 3 - 2 \times 1$ $1 = 3 - (5 - 3 \times 1) \times 1$ $= 3 \times 2 - 5 \times 1$ $1 = (13 - 5 \times 2) \times 2 - 5 \times 1$ $= 13 \times 2 - 5 \times 5$ This shows the inverse is -5 (or 8 which is $-5\ mod\ 13$)
$1562 = 1473 \times 1 + 89$ $1473 = 89 \times 16 + 49$ $89 = 49 \times 1 + 40$ $49 = 40 \times 1 + 9$ $40 = 9 \times 4 + 4$ $9 = 4 \times 2 + 1$ $1 = 9 - 4 \times 2$ $1 = 9 - (40 - 9 \times 4) \times 2$ $= 9 \times 9 - 40 \times 2$ $1 = (49 - 40 \times 1) \times 9 - 40 \times 2$ $= 49 \times 9 - 40 \times 11$ $1 = 49 \times 9 - (89 - 49 \times 1) \times 11$ $= 49 \times 20 - 89 \times 11$ $1 = (1473 - 89 \times 16) \times 20 - 89 \times 11$ $= 1473 \times 20 - 89 \times 331$ $1 = 1473 \times 20 - (1562 - 1473 \times 1) \times 331$ $= 1473 \times 351 - 1562 \times 331$ This shows the inverse is 351	$127 = 73 \times 1 + 54$ $73 = 54 \times 1 + 19$ $54 = 19 \times 2 + 16$ $19 = 16 \times 1 + 3$ $16 = 3 \times 5 + 1$ $1 = 16 - 3 \times 5$ $1 = 16 - (19 - 16 \times 1) \times 5$ $= 16 \times 6 - 19 \times 5$ $1 = (54 - 19 \times 2) \times 6 - 19 \times 5$ $= 54 \times 6 - 19 \times 17$ $1 = 54 \times 6 - (73 - 54 \times 1) \times 17$ $= 54 \times 23 - 73 \times 17$ $1 = (127 - 73 \times 1) \times 23 - 73 \times 17$ $= 127 \times 23 - 73 \times 40$ This shows the inverse is -40 (or 87 which is $-40\ mod\ 127$)

(2) Any number $a \geq 1$ has a unique factorization given by:

$$a = {p_1}^{a_1} {p_2}^{a_2} \cdots {p_n}^{a_n}$$

where $p_1, p_2, \cdots p_n$ are the first n primes.

Write an expression for the GCD of two numbers using the above representation of numbers.

$$a = {p_1}^{a_1} {p_2}^{a_2} \cdots {p_n}^{a_n}$$
$$b = {p_1}^{b_1} {p_2}^{b_2} \cdots {p_n}^{b_n}$$
$$GCD(a,b) = \prod_{i=1}^{n} {p_i}^{min(a_i, b_i)}$$

(3) Classical Ciphers

(a) What is a Caesar Cipher?

A Caesar Cipher is a substitution cipher and is also a stream cipher if the block size used is 1. The earliest version of the Caesar Cipher involved the substitution of an alphabet in the plaintext with another alphabet three places down. As an example, A would have the value of 1, and Z would have the value of 26. If the key k=3, then for the plaintext of ABC, the resulting ciphertext would be DEF.

A	B	C	=	A	B	C	=	D	E	F
1	2	3		1+3	2+3	3+3		4	5	6

(b) Explain differences between mono- and poly- alphabetic ciphers.

Mono-alphabetic cipher: Encoding using only one fixed alphabet (when the spaces between words are still there, these are fairly easy to break)

Poly-alphabetic cipher: Encoding using more than one alphabet, switching between them systematically.

(c) If you have a Caesar Cipher with key $k = 4$. Encrypt "MELBOURNE" using the key.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

$$k = 4$$
$$A \to E, B \to F, C \to G, \cdots Y \to C, Z \to D$$
$$MELBOURNE \to QIPFSYVRI$$

(d) Consider the affine Caesar cipher defined as follows. The encryption function is defined as: $C = E_{[a,b]}(p) = (ap + b)\ mod\ 26$, where p is the plain text and the tuple $[a, b]$ is the key.

(i) How many different keys are possible with the system?

b can take any value from integers modulo 26. However, a should have an inverse, i.e. a should belong to $\{1,3,5,7,9,11,15,17,19,21,23,25\}$. So totally there are $12 \times 26 = 312$ keys.

(ii) Derive a decryption function and determine what values of a and b are allowed, if this function exists.

$$p = (c - b)a^{-1}\ mod\ 26$$