HW1

1. Why hardware security is important? Briefly explain with an example.
    - Hardware security is important because if the hardware has vulnerabilities to it, it does not matter how much you secure the software running on it, the system is compromised. For example, take a side channel that leaks key bits through power traces when encrypting a message. In this case it does not matter if you improve the security of your encryption algorithm or make changes in software (with maybe a few exceptions) the system will be insecure.
2. In a Diffie-Helman key exchange, two parties securely communicate using asymmetric-key cryptography for a short time. They establish a symmetric key and use symmetric cryptography for the remainder of their communication. Explain why it is advantageous to switch to a symmetric algorithm instead of simply continuing to use the asymmetric algorithm.
    - Symmetric cryptography is faster to run because usually the keys are much shorter. Additionally, only one key gets which makes the process faster.
3. Consider the following scenario. An instructor wants to securely communicate with two TAs and a very large number of students. The instructor needs to communicate with the TAs on a daily basis (i.e., frequently) and needs to communicate with the students on a weekly basis (i.e., infrequently). It is acceptable for the TAs to be able to read each other's messages. However, each student cannot be allowed to read another student's message. For each of these two scenarios, what encryption scheme (Symmetric or Asymmetric Key Cryptography) would you recommend? Briefly justify your decision (consider types of keys, key distribution and management, and encryption & decryption time/bandwidth).
    1. Communication between the instructor and the TAs.
       a. Would you use Symmetric and Asymmetric Key Cryptography?
        - Yes, I would use both.
          b. Briefly justify your answer.
        - Because there is a small number of TA's so we will not need to manage a lot of keys (just one since they can read each others messages), like we would have to for the students' case. Since, the communication is also frequent it will be helpful to use the faster protocol to communicate (symmetric) once we establish session keys using the asymmetric protocol.
    2. Communication between the instructor and the students.
       a. Would you use Symmetric and Asymmetric Key Cryptography?
        - Only Asymmetric
          b. Briefly justify your answer.

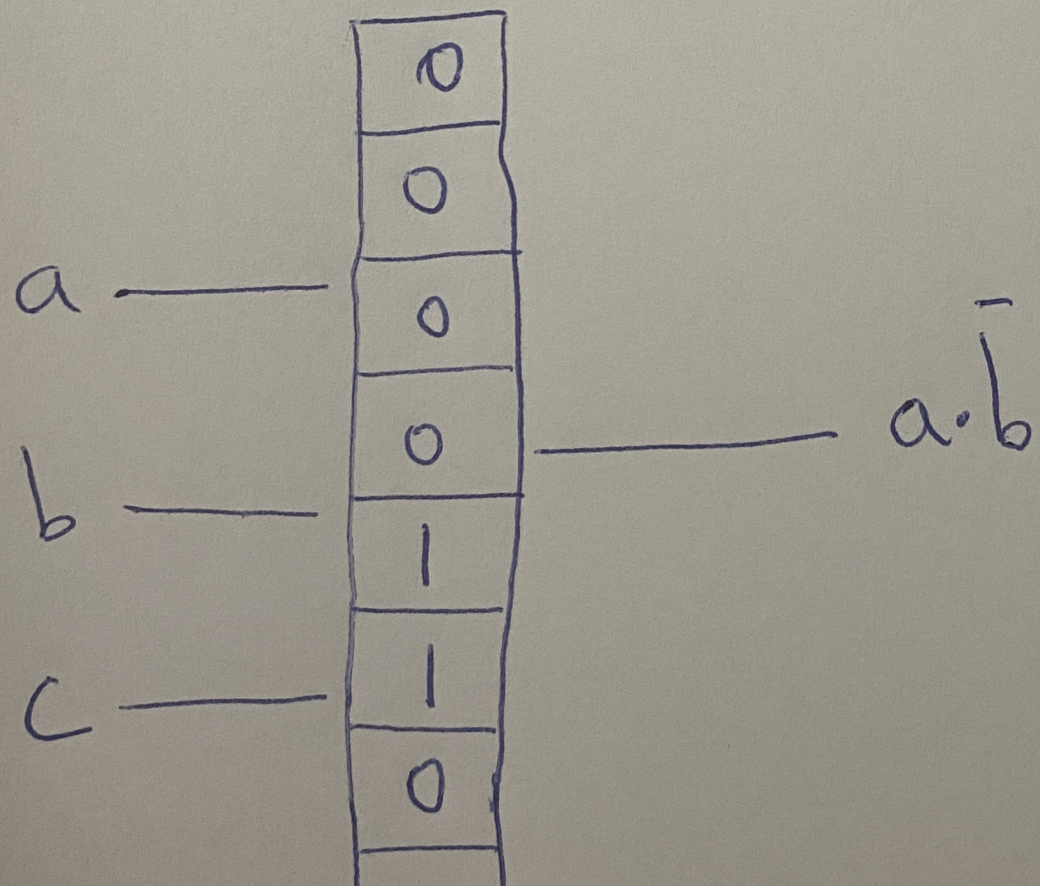
- Since there is a large number of students managing a large number of symmetric keys to be established between the professor and each students becomes a hard problem. Therefore, asymmetric cryptography is desired where the professor is able to share his public key with all the students to encrypt messages coming his way.

4. Describe the motives of the semiconductor industry to shift to a horizontal business model.
   - One of the main motives of the semiconductor industry to shift to a horizontal business model was to distribute the cost required to build and maintain (roughly every 2 years needs to be changed according to Moore's Law) the fabrication unit amongst several supply chain industries to reduce the expenses of one big firm. This would in turn reduce the manufacturing cost and enhance design reusability which are also incentives to move towards a horizontal business model.
5. The Data Encryption Standard (DES) is a symmetric-key algorithm that has a cipher key length of 56 bits. It was developed in the 1970s but is no longer considered to be secure. Advanced Encryption Standard (AES) is a newer symmetric-key algorithm that has cipher key lengths of 128,192 and 256 bits. AES became standard in the early 2000s to replace DES, and AES is still considered to be secure
   1. What is the fundamental reason why DES is no longer considered secure?
   - The key length of DES is 56 bits this requires a maximum of 2^{56} attempts to find the correct key with a brute-force attack. This is not enough to protect data with modern computers.
   2. Let us consider an attacker has access to a machine that can perform DES encryption at a speed of 2^{15} encryptions per second. Given the key size of 56 bits, how much time would it take an attacker to explore the entire key space (i.e., perform a brute force attack)?
   - To explore the entire key space the attacker would need 2^{41} seconds, approximately 69730 years
   3. What is the fundamental reason AES is still considered secure?
   - The fundamental reason why AES is still considered secure is the key size as opposed to DES (only 56 bits), AES allows the option to choose between 128, 192, or 265 bits for the key.
   4. Consider that the machine can also perform AES encryption at a speed of 2^{15} encryption per second. Given the key size of 128 bits, how long would it take for an attacker to explore the entire key space (i.e., perform a brute force attack)?
   - To explore the entire key space the attacker would need 2^{113} seconds, many many years.
6. For the given 3 input LUT, map the following functions using the minimum number of LUTs. (Must include the truth table)
   1. $a\bar{b}$

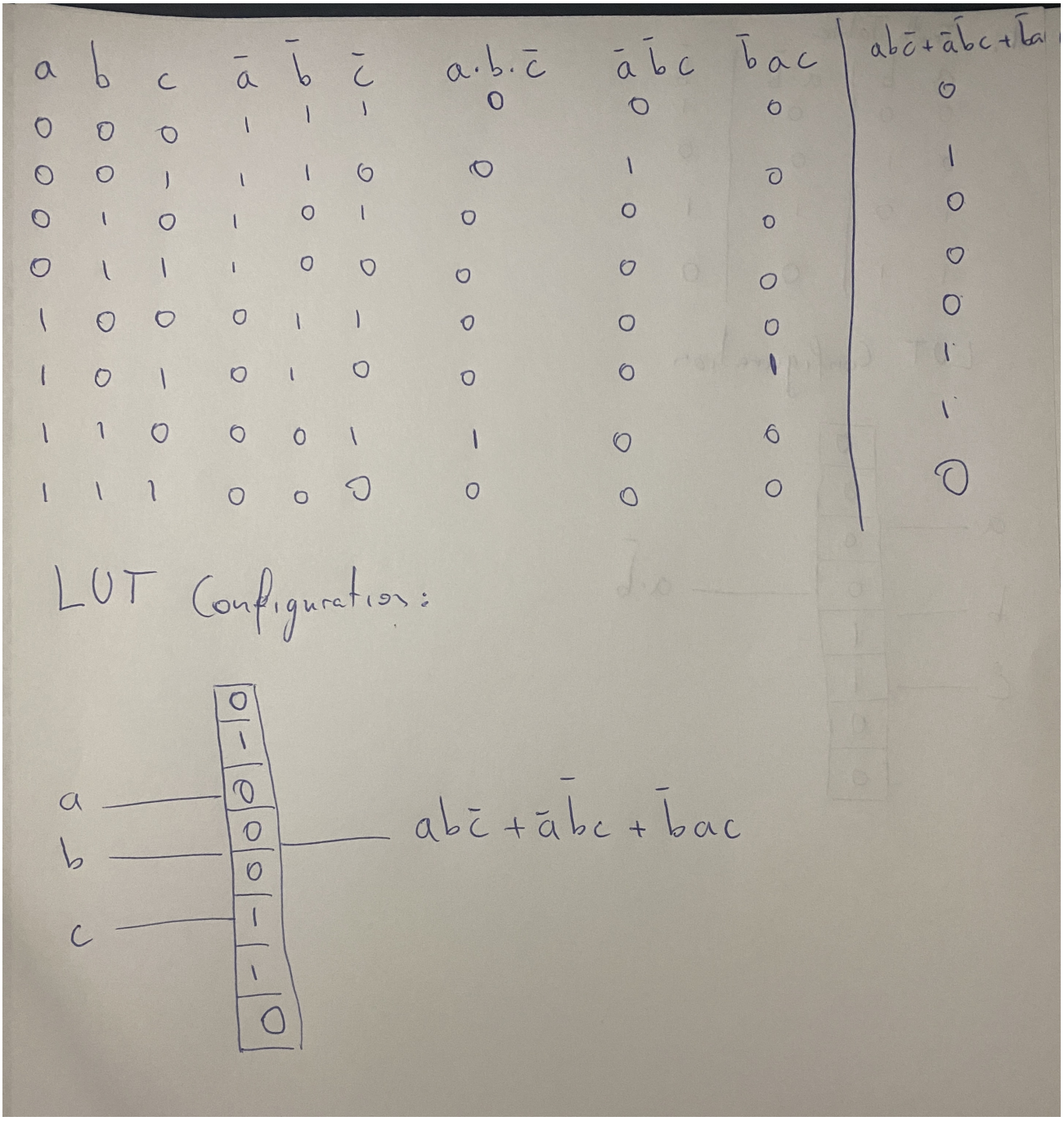
1. Truth Table

a	b	$a \cdot \bar{b}$	$\bar{b}$
0	0	0	1
0	1	0	0
1	0	1	1
1	1	0	0

LUT Configuration



2. $ab\bar{c} + \bar{a}\bar{b}c + \bar{b}ac$



7. Encrypt your last name using a Caesar cipher with key = 3. Show the details of your work.
   - Last name: Langus
     to encrypt it using Caesar's cipher with key = 3 we shift each letter alphabetically by 3.
     Example: A => D
     Following this for my last name:
     Langus => Odqjxv (ignoring case)
8. The following figure shows a simplified diagram of the hardware design flow.

- Briefly (3-4 sentences each) describe the trust issues between:
  1. IP Vendor and System Integrator

- IP overuse: The SoC designer may produce more ICs and report a lesser amount to the IP owners to reduce the licensing cost. At the same time, the SoC designer may illegally use an IP that was licensed to be used in a different design.

2. System Integrator and IP Vendor

- IP piracy: A SoC designer may legally purchase a 3PIP core from an IP vendor and then make clones, or illegitimate copies of the original IP.

3. System Integrator and Foundry.

- IC overproduction: Untrusted foundries and assemblies may produce more than the number of chips they are contracted to manufacture.

9. For the given plain text and key, calculate the add round key, sub-bytes, and shift rows of the first round of AES encryption (NEXT PAGE FOR SOLUTION)

9.

$$\text{Text} = \begin{bmatrix} fe & aa & 25 & e9 \\ a9 & 02 & 98 & 27 \\ f6 & fe & 96 & be \\ ee & f9 & 4c & 9c \end{bmatrix} \quad \text{Key} = \begin{bmatrix} 98 & 68 & 6e & 6c \\ a0 & 2a & dd & 46 \\ 5c & d1 & 3a & 06 \\ da & 3c & 36 & ba \end{bmatrix}$$

Add round key:

$$\text{In} = \begin{bmatrix} 66 & c1 & 4b & 85 \\ 09 & 28 & 45 & 61 \\ aa & 2f & ac & b8 \\ 34 & c5 & 7a & 26 \end{bmatrix}$$

Sub bytes:

$$\begin{bmatrix} 33 & 78 & B3 & 97 \\ 01 & 34 & 6E & EF \\ aC & 15 & 91 & 6C \\ 18 & A6 & da & F7 \end{bmatrix}$$

(See S-Box)

Shift rows:

$$\begin{bmatrix} 33 & 78 & b3 & 97 \\ 34 & 6E & EF & 01 \\ 91 & 6C & aC & 15 \\ f7 & 18 & A6 & da \end{bmatrix}$$