CS4732/5732 **Cryptography** **Summer 2020**

Project #2 [70 points]

Due date is Thursday, July 20th

Overview:

This is the math option for our project2. It involves theoretical and practical calculations involving block ciphers and pseudorandom number generation.

1) Considering CTR mode, suppose that you know the plaintext block and the counter value. Given the ciphertext, you can determine easily what the output of the encryption function is. Show the calculation.
2) Suppose you wanted to try a meet-in-the-middle attack on double AES using 128 bit keys.
    a. Exactly how much storage would you need for it, in gigabytes.
    b. How many total encryption operations would you expect to have to do in order to complete your attack?
    c. Calculate how much more storage you would need if we went to 196 bit keys.

ANSWER FOR 1,2 ARE BELOW

Brandon London 7/10/20

1) To encrypt a series of plaintext blocks, Lets Assume $P_1, P_2, \ldots P_n$ using block cipher $E^{(e)}$ operating in Electric code book mode, then each cipher text block $C_1 C_2 \ldots C_n$ is computed as $C_i = E_k(P_i)$

If a cipher text block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected. In ECB mode, altering a ciphertext block only affects a single plaintext block.

2) A) The size of storage required is 2^{64} bits $= 1.84 \times 10^{19}$

1 giga bit $= 8 \times 10^9$ so storage in gb $= 1.84 \times 10^{19} / 8 \times 10^9$

Storage $= 2.3 \times 10^8$

b) Number of operations for AES is 2^{64} and double will take double the operations 2×2^{64}

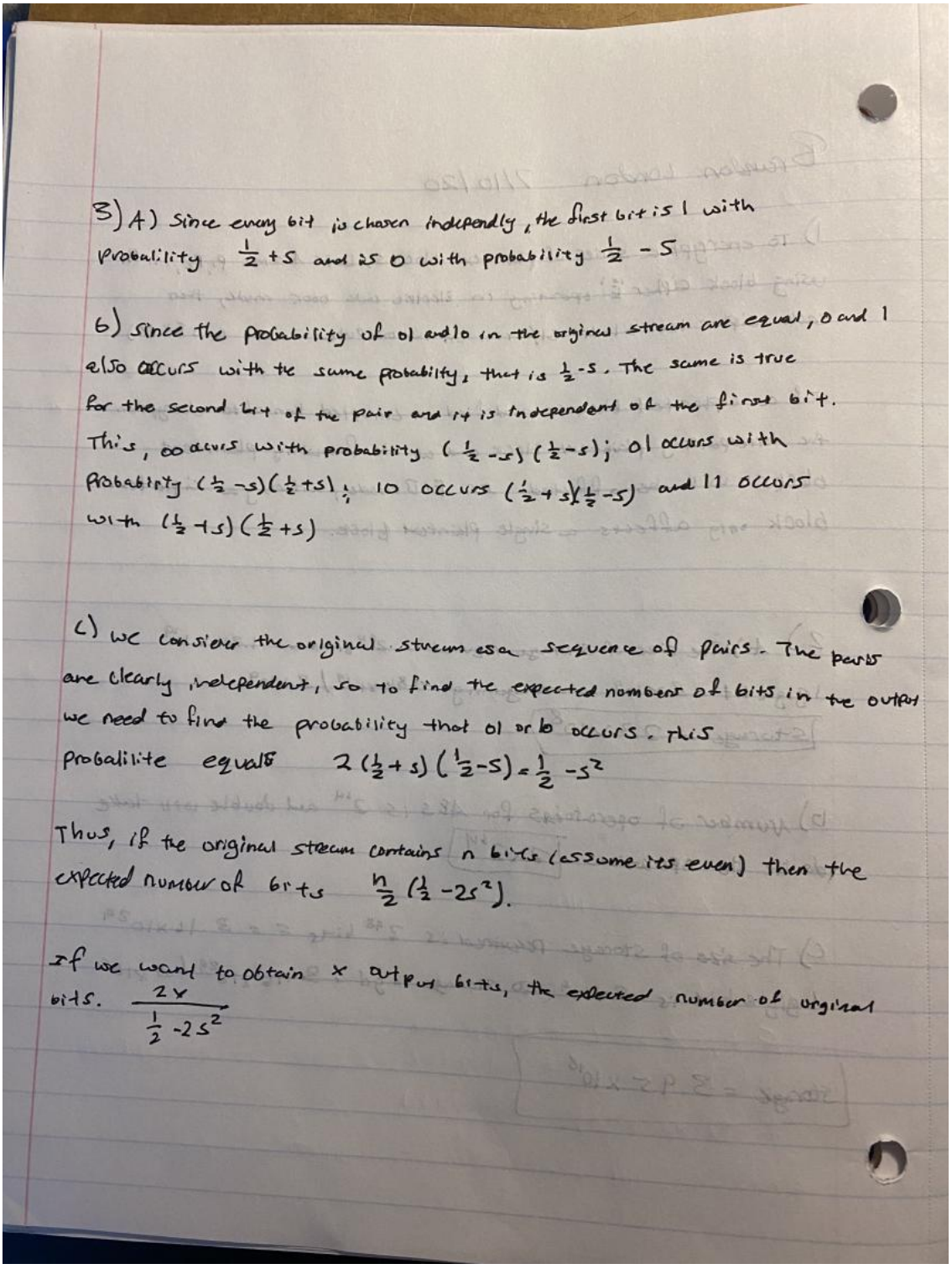
c) The size of storage required is 2^{48} bits $= 3.16 \times 10^{29}$

1 giga bit is 8×10^9 so storage in gb $= 3.16 \times 10^{29} / 8 \times 10^9$

Storage $= 3.95 \times 10^{18}$

3) Suppose you have a true bit generator where each bit in the generated stream has the same probability of being a 0 or a 1 as any other bit in the stream and that bits are not correlated. However, the bit stream is biased. In particular, the probability of a 1 is 0.5 + a. and the probability of a 0 is 0.5 – a, where $0 < a < 0.5$. One way to condition this data is to examine the bit steam for nonoverlapping pairs. Discard all the 00 and 11 pairs. Replace each 01 pair with 0 and each 10 pair with 1.

a) What is the probability of each pair in the original sequence?
b) What is the probability of occurrence of 0 and 1 in the modified sequence?
c) What is the expected number of input bits to produce x output bits?



3) A) Since every bit is chosen independly, the first bit is 1 with probability $\frac{1}{2}+s$ and is 0 with probability $\frac{1}{2}-s$

b) since the probability of 01 and 10 in the orginal stream are equal, 0 and 1 also occurs with the same probabilty, that is $\frac{1}{2}-s$. The same is true for the second bit of the pair and it is independent of the first bit. This, 00 occurs with probability $(\frac{1}{2}-s)(\frac{1}{2}-s)$; 01 occurs with probability $(\frac{1}{2}-s)(\frac{1}{2}+s)$; 10 occurs $(\frac{1}{2}+s)(\frac{1}{2}-s)$ and 11 occurs with $(\frac{1}{2}+s)(\frac{1}{2}+s)$

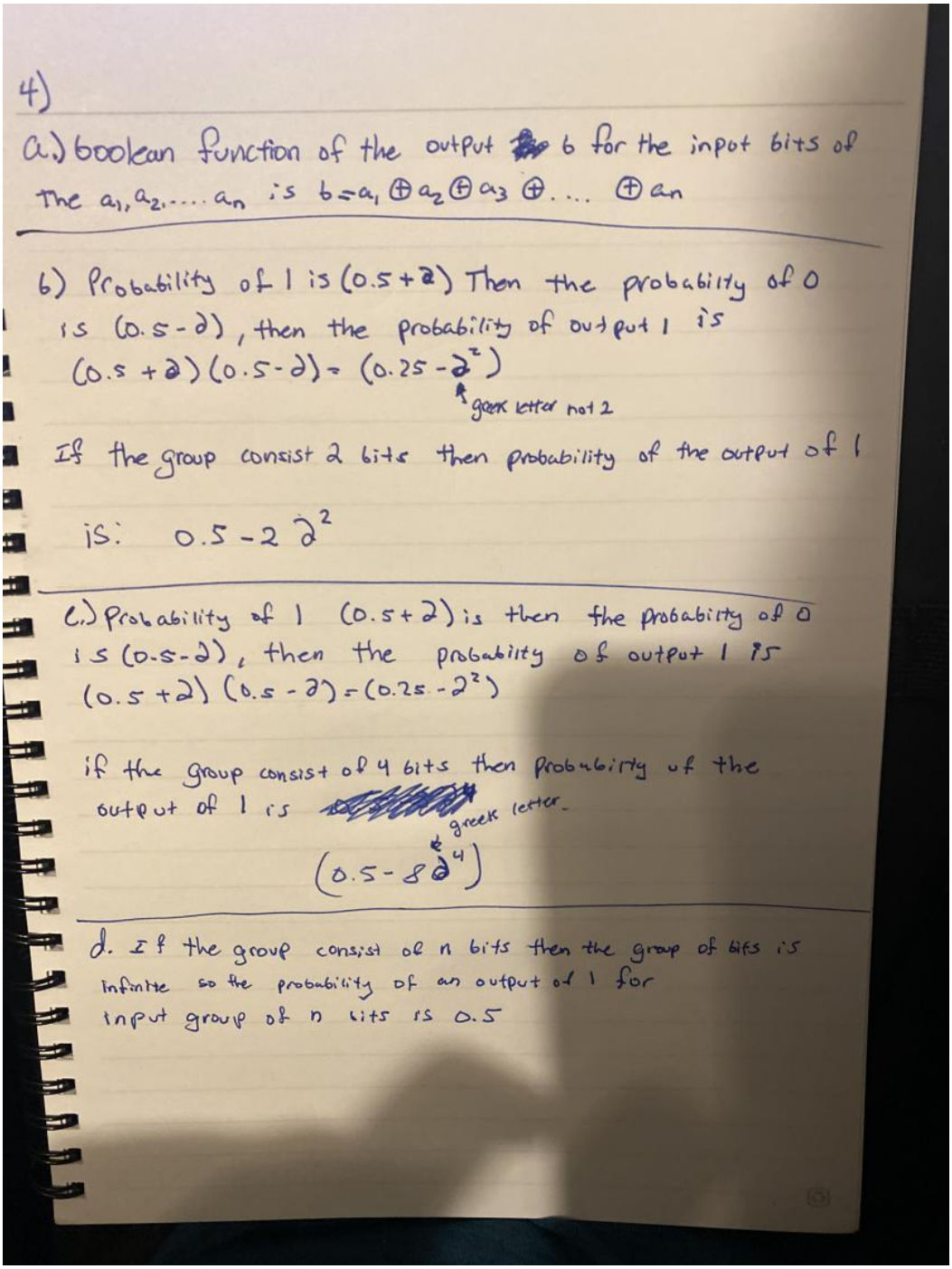
c) we consider the original stream as a sequence of pairs. The pairs are clearly independent, so to find the expected nombers of bits in the output we need to find the probability that 01 or 10 occurs. this probalilite equals $2(\frac{1}{2}+s)(\frac{1}{2}-s) = \frac{1}{2}-s^2$

Thus, if the original stream contains n bits (assume its even) then the expected number of bits $\frac{n}{2}(\frac{1}{2}-2s^2)$.

if we want to obtain x output bits, the expected number of original bits. $\frac{2x}{\frac{1}{2}-2s^2}$

4) Another approach to conditioning is to consider the bit stream as a sequence of nonoverlapping groups of n bits each and output the parity of each group. That is, if a group contains an odd number of ones, the output is 1; otherwise the output is 0.
    a. Express this operation in terms of a basic Boolean function
    b. Assume that the probability of a 1 is 0.5 + a, where $0 < a < 0.5$. If each group consists of 2 bits, what is the probability of an output of 1.
    c. If each group consists of 4 bits, what is the probability of an output of 1?
    d. Generalize the result to find the probability of an output of 1 for input groups of n bits.

Answer IS below



4)

a.) boolean function of the output b for the input bits of the $a_1, a_2, \ldots a_n$ is $b = a_1 \oplus a_2 \oplus a_3 \oplus \ldots \oplus a_n$

b) Probability of 1 is $(0.5+\partial)$ Then the probability of 0 is $(0.5-\partial)$, then the probability of output 1 is $(0.5+\partial)(0.5-\partial) = (0.25-\partial^2)$

↑ greek letter not 2

If the group consist 2 bits then probability of the output of 1 is: $0.5 - 2\partial^2$

c.) Probability of 1 $(0.5+\partial)$ is then the probabilty of 0 is $(0.5-\partial)$, then the probability of output 1 is $(0.5+\partial)(0.5-\partial) = (0.25-\partial^2)$

if the group consist of 4 bits then probability of the output of 1 is

greek letter

$(0.5 - 8\partial^4)$

d. If the group consist of n bits then the group of bits is infinite so the probability of an output of 1 for input group of n bits is 0.5

5) Suppose you have the generator $X_{n+1} = (aX_n) \bmod 2^4$.

a. What is the maximum period obtainable from the following generator? Note that it is not 16. You can either try and calculate this or figure it out manually by trying all possible values of a.

b. What should be the value of a?

c. Are there any restrictions required on the seed?

5) A maximum period is $2^{4-2} = 2$

8) A must be 5 or 11

c) yes. The seed must be odd.