**Question 1**

Mistakes and Proposed Solutions

1. Alice key generation is computed wrongly, it should have been computed as follows, s = *B****a*** mod *p.* The reason for this is because it should have been A=[a]G, which is a function for publishing the public key process and not
2. Alice computes E=[e]G is wrong, the whole process requires Alice to compute as follows (A, ga). Additionally, Alice and Bob compute need verify the key signature as follows r=R(gxy). The key verification process is wrongly computed i.e and should be verified as shown above.
3. Alice computes the common secret key kAB =hash (kAB ||a||e) is wrong, this will amount to invalid key and signature verification will not go through. Verification must have a prime order as indicated below

A=GH1(r,a), A=G1(a,r)

The signature is invalid based on the explanations given above

**Question 2**

g(x) is a collusion resistant function since it provides a combination of properties with cryptographic hash functions. h:{0,1}n→{0,1}m is a collision-resistant hash function. Having a one-bit compressing collision resistance function we can obtain polynomial-length compressing collision *h* resistance function by repeatedly applying *h*. Observe that this method is not multi-message secure for digital signatures because *m* and *h*(m) hash to the same value. The collision resistance function can be further explained through the introduction of the adversaries by assuming the following

Advcrf(A) = Pr[Fk(X) =Fk(X′) ∧ X6=X′:k$← K; (X, X′)$← A(k). In this function we define collision finding advantage of the adversary *A* against *F*. This forms the basis of concluding that it is collusion resistant function.

About one-wayness function, an integrity service is normally obtained by running one-way function on the message through a cryptographic key, this is mostly used in message authentications

**Question 3**

For the issue of using the smartphone to trace COVID-19 patients, cryptographic techniques can be adopted to secure the communication. The most ideal solution that would enhance privacy and security is by the use of highly secure mobile phone communications that provides security against eavesdropping and electronic surveillance. The use of encryption in the smartphones can protect phone communication from any form of interception through the use of algorithms to encrypt the signals. Smartphones with the chip that can handle both encryption and decryption can ensure that the communication between the surveillance team is secure. In this case, two algorithms are programmed in the chip, that uses a key exchange algorithm for key agreement protocol, as well as asymmetric key algorithm that is meant for voice encryption.

In ensuring that the cryptographic primitives are well applied in the smartphone communication, several secure practices are available. Such practices include the use of AES algorithm and Hash-based message authentication to guarantee the integrity of communication and degree of accountability. Additionally, the protocol used must authenticate the public key since we cannot depend on the certificates, this is mostly done by challenging the server to decrypt secret key used in the communication

**Question 4:**

 In linear mappings, it makes use of a matrix as a cipher to encode a message or communication, and it's extremely difficult to break when a large matrix is used. The receiver of the message decodes it using the inverse of the matrix. This first matrix is called the encoding matrix and its inverse is called the decoding matrix. Non-linear mappings or functions are known to have the optimal properties for offering resistance against differential cryptanalysis, and have since an object of intensive study by many mathematicians.

1. The first step in the problem given is a non-linear function .i.e.

This reason of the above being a non-linear mappings or function is because it is differentially uniform and is exploited in the form of

Which forms the basis of the theorem.

1. Both step 2 and step 4 are also non-linear functions/ mappings, that is

The reason why the above steps are non-linear because in cipher message, looping occurs in no particular order or linear form

1. Step 3 and step 5 have linear mapping/ functions as shown below

The rationale behind the two functions being linear, is because they satisfy the linear mapping rule, which is