CIS-481: Introduction to Information Security

Module 10 - Cryptography

Exercise #8

Team: 5

Participants: Sam Martin, Abril Beascoechea, Charles Degboe, Nicholas Zhang, Ricardo Portillo

Logistics

A. Get together with other students on your assigned **Team** in person and/or virtually.

B. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning and may impact your performance on assessments, especially with respect to the essay questions.

C. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1 *(8 points)*

Using the Vigenère Square on p. 389 and the key **CYBERSECURITY**, decrypt the following ciphertext message:

GLDVPHXKIEQLDWL

Be sure to show or describe your work decrypting the message.

ENCRYPTIONISFUN

To decrypt this message you would follow the pattern for each letter shown. First you have to compare the ciphertext and the keyword, with that you can start decrypting. You would find "C' on the Vigenere square, and then find the letter "G" in that row. (these are the first letters of the keyword and ciphertext) The letter "G" is located in column "E" so E would be the first letter. You then would repeat this process.

Problem 2 *(7 points)*

Contrast *asymmetric* encryption with *symmetric* encryption. What drawbacks to symmetric and asymmetric encryption used alone are resolved by using a hybrid method like Diffie-Hellman?

Asymmetric encryption uses two different but related keys, either key can be used to encrypt or decrypt a message but it can't be the same key for both. Symmetric, on the other hand, uses a single key both to encrypt and decrypt the message.

Diffie-Hellman protects data from exposure to third parties, which resolves the problem of security when using asymmetric encryption for sending messages. The hybrid method also allows two people to exchange the key, resolving the drawback to symmetric encryption of key distribution.

Problem 3 *(10 points)*

If Alice wants to send a message to Bob such that Bob would know that the message *had to come from Alice* **AND** Alice could be certain that *only Bob could decrypt* it, show the necessary steps and keys to use with *public key encryption*. Use a diagram to explain the process. You may use two rounds of encryption in sequence or explicitly add a digital signature with a hash.

Alice and Bob can use both public-key encryption and digital signatures combined to achieve secure communication.

A private key and the corresponding public key are generated for Bob. The public key is sent to Alice and everybody else who wants to send Bob some encrypted messages, but the private key is held by Bob in secret.
Key generation makes Alice generate a secret private key and another public key corresponding to it. In the same manner, Alice distributes her public key to Bob, or any desired person, who wants to send her encrypted messages, but she keeps its private key secret.

Encryption of Messages:
Alice and Bob communicate. She initiates the process by getting the public key from Bob.

We use Bob's public key to encrypt Alice's message, such that only Bob can use the corresponding private key to decrypt the message. The message is then encrypted and relayed via Alice for sending to Bob.
She wants Bob to be able to verify that the communication indeed originated from her even before sending the encrypted message; Alice therefore attaches a digital signature to the message.

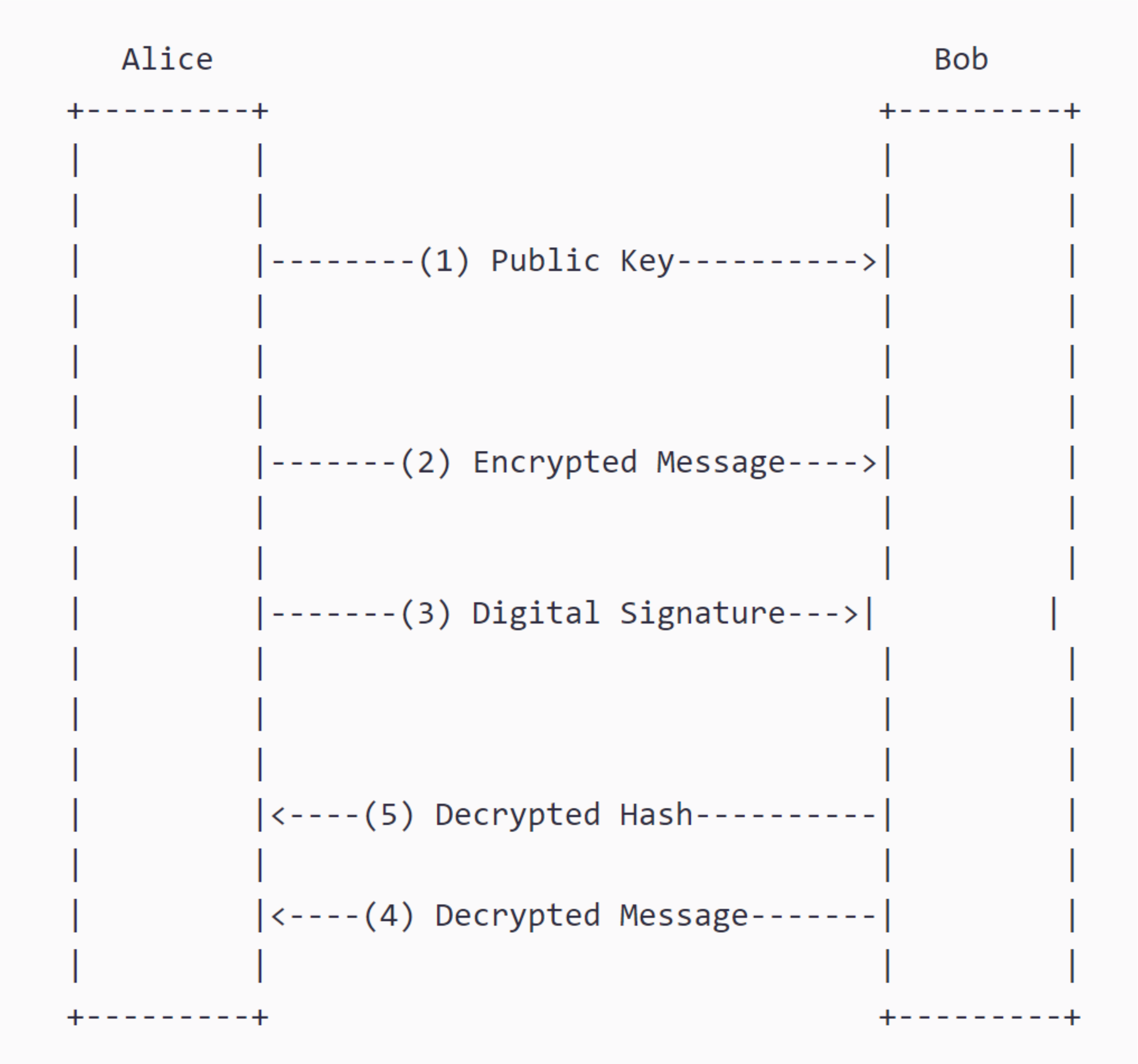
Using a hash cryptographic function, Alice hashes (digests) the message. She encrypts the hash with her private key. The electronic signature results. The electronic signature generated by Alice is added to the encrypted communication.

Sending a message:
What Bob receives is the encrypted message with the digital signature of Alice.
Receiving and Attending to Messages:
The original message is sent. The original hash, which was unveiled by decrypting the digital signature with his private key, is revealed by Bob using his private key, with it being able to unlock Alice's original message from the encrypted message.

Bob applies the same hash function that Alice had used while calculating independently the hash of the received message.

Bob compares the hash produced with the hash digital signature that had been decrypted. If they match, it confirms the authenticity of the message and proves beyond a reasonable doubt that Alice is the source of that particular message.

Here is the diagram below:



```
   Alice                                       Bob
+---------+                                 +---------+
|         |                                 |         |
|         |                                 |         |
|         |--------(1) Public Key---------->|         |
|         |                                 |         |
|         |                                 |         |
|         |                                 |         |
|         |-------(2) Encrypted Message---->|         |
|         |                                 |         |
|         |                                 |         |
|         |-------(3) Digital Signature--->|         |
|         |                                 |         |
|         |                                 |         |
|         |                                 |         |
|         |<----(5) Decrypted Hash----------|         |
|         |                                 |         |
|         |<----(4) Decrypted Message-------|         |
|         |                                 |         |
+---------+                                 +---------+
```

In the first step, Alice requests and receives the public key of Bob. Alice, using the received public key of Bob, uses the second message to encrypt the text. Step 3: Alice digitally signs the message, this is Alice's first step; she digitally signs the message by creating a digital signature for it and encrypting the hash of the message using her private key and attaches it to the encrypted message. Step 4: Bob decrypts the digital signature using Alice's public key to obtain the original hash. Step five: Bob decrypts the coded message by using his private key to get the original message from Alice. Bob further goes ahead and calculates the hash of the message received to compare with that of the decrypted message to verify the authenticity and the source of the communication. Alice makes sure that the message can only, obviously, be decrypted by Bob's public key and uses the concept of digital signature and encryption together: Bob verifies that the request truly comes from Alice.