1) How Would Alice Send the Message?

firstly Alice Would need to encrypt the message M1 using Bobs public key Pu(B)
$E\_\{Pu(B)\}(M1)$.

Secondly, Alice Sends the encrypted Message over the internet. Bob then Receives the message from Alice. Bob then needs to decrypt the message using his private key Which is:
$D\_\{Pr(B)\}(E\_\{Pu(B)\})(M1)$, Bob Can now read the Message.

Decrypt key Encrypted key Message

2) Let us denote the message Alice sent As M-3. How would Bob decipher the message?

Bob Would use his private key to decrypt the encrypted Message $E\_\{Pu(B)\}(M3)$:
$D\_\{Pr(B)\}(E\_\{Pu(B)\}(M3))$. After decrypting the message Bob Will be able to Read the original Message that Alice encrypted.

3) In this situation, Alice does not Care if anyone Can Read her message. But she does Care no one in the middle Can change the message. Let us denote the Message As M-2

To make Sure that the message has not been modified by anyone, Alice Can use a digital Signature to Sign the message.
1) Alice Creates a digest of the message using A hash function. $H(M2)$
2) Alice Will need to encrypt using her private Key; $E\_\{Pr(A)\}(H(M2))$
3) Alice Attaches the digest to the encrypted Message. $M2 \,||\, E\_\{Pr(A)\}(H(M2))$
4) finally, Alice Can now Send that Message to Bob over the internet.

4) What Would Bob do to verify that the message indeed Came from Alice?

Bob Would Receive the Message, Bob Would then need to Seperate the digest from the original Message. Bob would then decrypt the encrypted Message $D\_\{Pu(A)\}E\_\{Pr(A)\}(H(M2))$
Bob Creates a digest of the Received Message using the Same hash function as Alice $H(M2)$
As a Result Bob Can Compare the decrypted digest With the digest of the Received Message, if they are the Same Bob knows the message had not been tampered with.