Outputs for Reflection Attack in Original Needham-Schroeder Protocol (With ECB and CBC)

Output for Alice:

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS E:\Network Security CS 6490\Programming Assignment\pkg>  & 'C:\Program Files\Eclipse Adoptium\jdk-17.0.6.10-hotspot\bin\java.exe' '-XX:+ShowCodeD
etailsInExceptionMessages' '-cp' 'C:\Users\heman\AppData\Roaming\Code\User\workspaceStorage\d35b161259cea1df3985c80662149c8e\redhat.java\jdt_ws\pkg_
f44b4f6f\bin' 'AliceReflection'
AliceReflection has started.
Alice established connection with Bob.
Alice established connection with KDC.
n1: -715783531087410409 n1 received: -715783531087410409
idBob: 8019351793 idBob received:8019351793
ABKey: 7wB_U4T0z2uugbpqa9CuEWWC
ticketToBob: QhrYGAPWtl8sUf9yWV6iE1UGUKXNR5JanBsqFrMZtGF9yiRqVloF6A==
n2 is: -71226377745728920
message4: heG9qI6K9z/LLlAYMqYXwPMop+6rRo8h;JWG/7r/i8IMlR1IJUKA5u1oi4fB8Mbjz
n2-1: -71226377745728921
N2 and N2-1 is verified at Alice.
Initiating CHEAT mode... Unleashing Trudy!
Trudy used same ticket and starts a new conversation with Bob.
While sending message4 Trudy uses data extracted KAB{N3} from the initial connection with Bob.
message4 encrypted: fULnxyGdN8Yr9g/o5Cd0C3nl05jkzuS3JWG/7r/i8IMlR1IJUKA5u1oi4fB8Mbjz
Bob now verifies and authenticates Alice. Check Bob's output window.

Let us now change the protocol to CBC instead of ECB. And reattempt the reflection attack.
message4CBC: heG9qI6K9z/LLlAYMqYXwPMop+6rRo8h;JWG/7r/i8IMlR1IJUKA5u1oi4fB8Mbjz

Reflection attack failed in case of TripleDES with CBC.

An exception arises as the characters of Kab{N3} extarcted do not make sense. br.readLine() expects only string objects.
More details of why the connection closed: Connection reset
PS E:\Network Security CS 6490\Programming Assignment\pkg>
```

Output for Bob:

```
PS E:\Network Security CS 6490\Programming Assignment\pkg>  & 'C:\Program Files\Eclipse Adoptium\jdk-17.0.6.10-hotspot\bin\java.exe' '-XX:+ShowCodeD
etailsInExceptionMessages' '-cp' 'C:\Users\heman\AppData\Roaming\Code\User\workspaceStorage\d35b161259cea1df3985c80662149c8e\redhat.java\jdt_ws\pkg_
f44b4f6f\bin' 'BobReflection'
BobReflection has started.
Connection established with Alice!
Ticket received: QhrYGAPWtl8sUf9yWV6iE1UGUKXNR5JanBsqFrMZtGF9yiRqVloF6A==
Encrypted n2: heG9qI6K9z/LLlAYMqYXwIghoTIUEqh8
ABKey: 7wB_U4T0z2uugbpqa9CuEWWC
n2 generated is: -71226377745728920
message4 encrypted, in hexadecimal is:

68 65 47 39 71 49 36 4B 39 7A 2F 4C 4C 6C 41 59 4D 71 59 58 77 50 4D 6F 70 2B 36 72 52 6F 38 68 4A 57 47 2F 37 72 2F 69 38 49 4D 6C 52 31 49 4A 55 4
B 41 35 75 31 6F 69 34 66 42 38 4D 62 6A 7A Connected to Trudy aka Alices dupe.
Bob receives KAB{N2-1,N3} and is expected to send back KAB{N3-1}.
Bob computes the vlaue of KAB{N3-1} and sends it back to Alice.
message5 encrypted, in hexadecimal is:

4A 57 47 2F 37 72 2F 69 38 49 4D 6C 52 31 49 4A 55 4B 41 35 75 7A 6E 67 4F 56 57 39 62 74 62 41 N3-1 and N3 is verified at Bob. Reflection was succe
ssful.

Initiating a reattempt of the reflection attack using CBC instead of ECB.
message4 encrypted CBC, in hexadecimal is:

68 65 47 39 71 49 36 4B 39 7A 2F 4C 4C 6C 41 59 4D 71 59 58 77 48 4B 52 36 57 37 57 70 6A 56 4F 6E 58 73 67 42 42 2B 7A 4F 74 45 6F 49 70 61 45 58 5
2 58 63 35 67 3D 3D Message 4 trimmed: [B@2401f4c3

Bob was unable to resolve the value of N3 as the protocol used was CBC in TripleDES. Reflection attack has failed. Printing the exceptions:
The decryption failed due to improper format. Returning empty string. More details on why the decryption failed: Illegal base64 character -2a
Using CBC saved us from authenticating Alice's dupe.
An exception arises as the received Kab{N3} extracted by Trudy does not make sense to the algorithm as it is simply a trimmed encrypted string.
In continuation, due to the result of the first exception, the resulted decrypted string cannot be convert to a long.
PS E:\Network Security CS 6490\Programming Assignment\pkg>
```

Output for KDC: