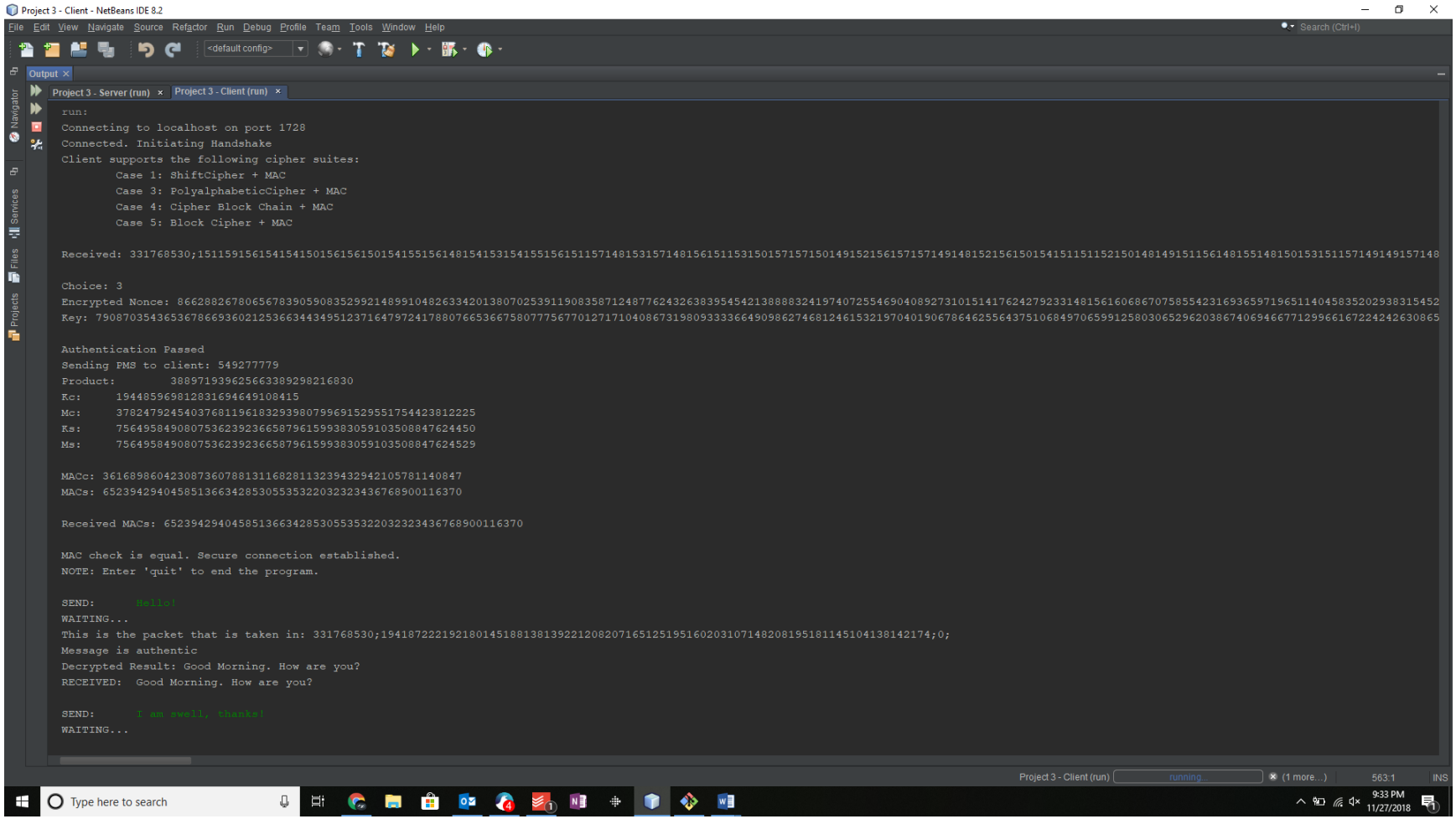
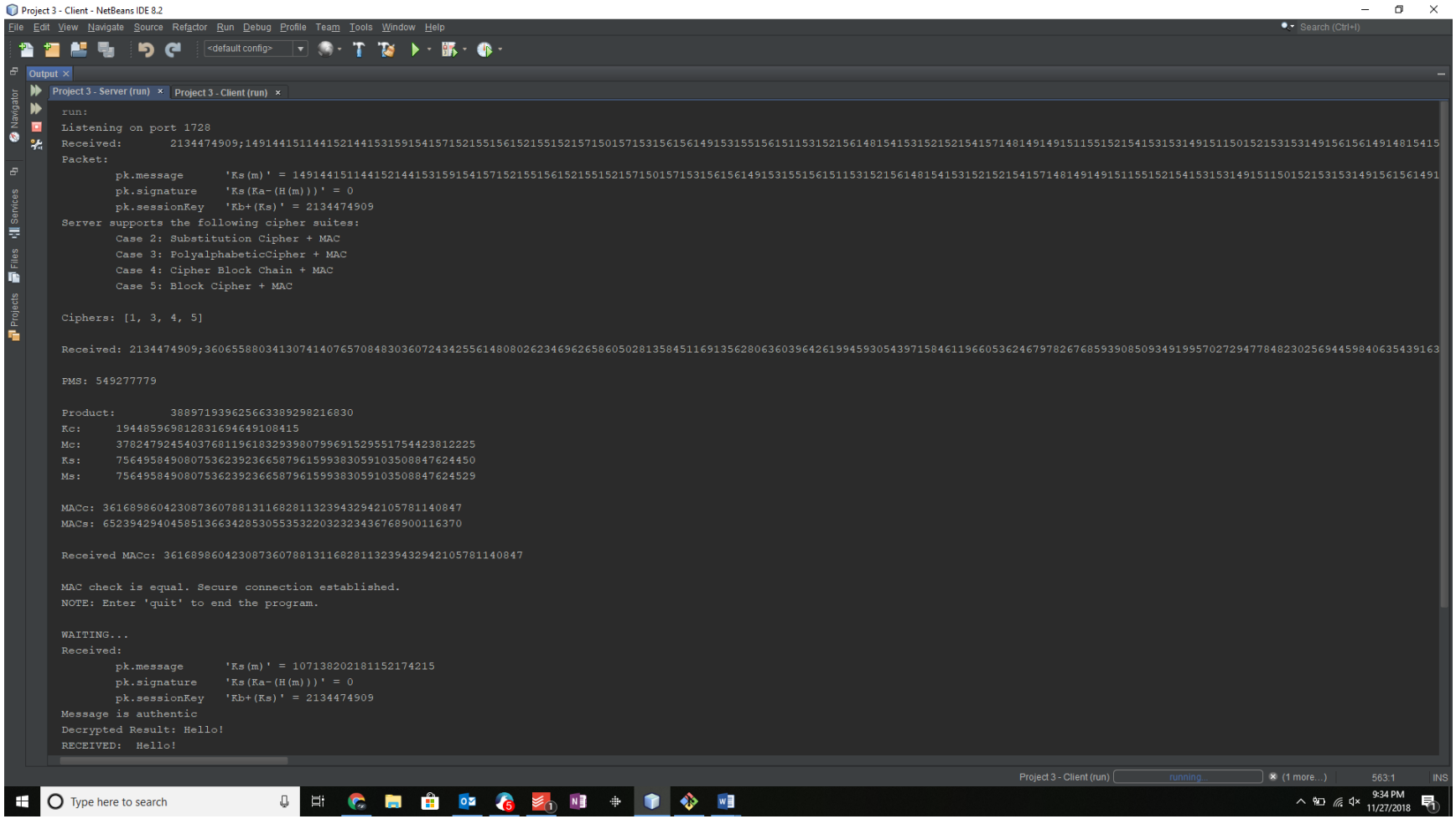
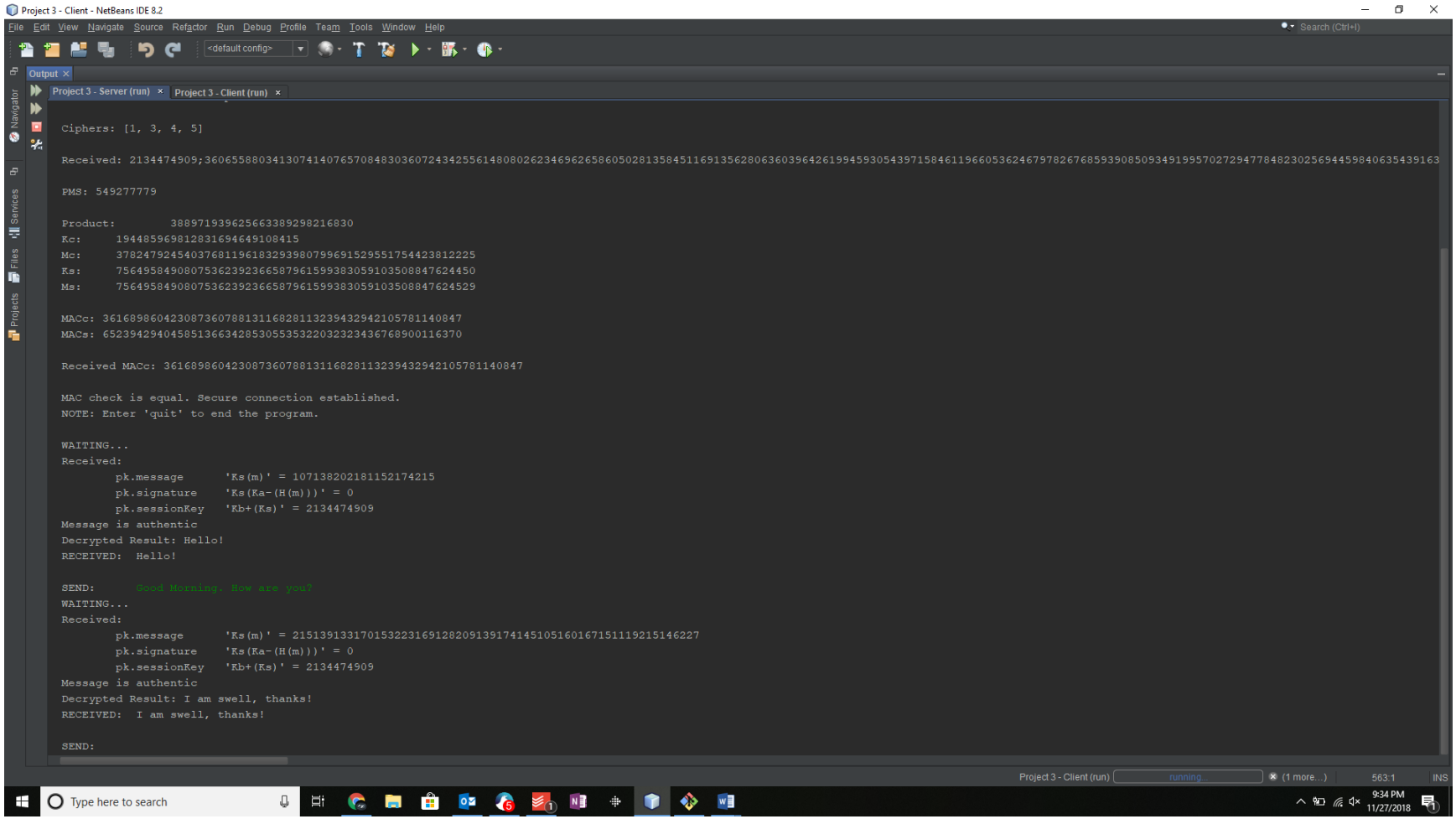

Project 3 - Client - NetBeans IDE 8.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Search (Ctrl+I)
<default config>
Output
Project 3 - Server (run)
Project 3 - Client (run)
run:
Connecting to localhost on port 1728
Connected. Initiating Handshake
Client supports the following cipher suites:
Case 1: ShiftCipher + MAC
Case 3: PolyalphabeticCipher + MAC
Case 4: Cipher Block Chain + MAC
Case 5: Block Cipher + MAC
Received: 331768530;151159156154154150156156150154155156148154153154155156151157148153157148156151153150157157150149152156157157149148152156150154151151521501481491511561481551481501531511571491491571481
Choice: 3
Encrypted Nonce: 866288267806567839059083529921489910482633420138070253911908358712487762432638395454213888832419740725546904089273101514176242792331481561606867075855423169365971965114045835202938315452
Key: 790870354365367866936021253663443495123716479724178807665366758077756770127171040867319809333366490986274681246153219704019067864625564375106849706599125803065296203867406946677129966167224242630865
Authentication Passed
Sending PMS to client: 549277779
Product: 388971939625663389298216830
Kc: 19448596981283169464910841 5
Mc: 37824792454037681196183293980799691529551754423812225
Ks: 75649584908075362392366587961599383059103508847624450
Ms: 7564958490807536239236658796159938305910350884762 4529
MACc: 361689860423087360788131168281132394329421057811408 47
MACs: 652394294045851366342853055353220323234367689001163 70
Received MACs: 652394294045851366342853055353220323234367689001163 70
MAC check is equal. Secure connection established.
NOTE: Enter 'quit' to end the program.
SEND: Hello!
WAITING...
This is the packet that is taken in: 331768530;194187222192180145188138139221208207165125195160203107148208195181145104138142174;0;
Message is authentic
Decrypted Result: Good Morning. How are you?
RECEIVED: Good Morning. How are you?
SEND: I am swell, thanks!
WAITING...
Project 3 - Client (run) running... (1 more...)
563:1
INS
Type here to search
9:33 PM
11/27/2018


Project 3 - Client - NetBeans IDE 8.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Search (Ctrl+I)
<default config>
Output
Project 3 - Server (run)
Project 3 - Client (run)
run:
Listening on port 1728
Received: 2134474909;1491441511441521441531591541571521551561521551521571501571531561561491531551561511531521561481541531521521541571481491491511551521541531531491511501521531531491561561491481541
Packet:
pk.message 'Ks(m)' = 1491441511441521441531591541571521551561521551521571501571531561561491531551561511531521561481541531521521541571481491491511551521541531531491511501521531531491561561491
pk.signature 'Ks(Ka-(H(m)))' = 0
pk.sessionKey 'Kb+(Ks)' = 2134474909
Server supports the following cipher suites:
Case 2: Substitution Cipher + MAC
Case 3: PolyalphabeticCipher + MAC
Case 4: Cipher Block Chain + MAC
Case 5: Block Cipher + MAC
Ciphers: [1, 3, 4, 5]
Received: 2134474909;3606558803413074140765708483036072434255614808026234696265860502813584511691356280636039642619945930543971584611966053624679782676859390850934919957027294778482302569445984063543916
PMS: 549277779
Product: 38897193962566338929821 6830
Kc: 19448596981283169464910 8415
Mc: 37824792454037681196183293980799691529551754423812225
Ks: 75649584908075362392366587961599383059103508847624450
Ms: 75649584908075362392366587961599383059103508847624529
MACc: 36168986042308736078813116828113239432942105781140847
MACs: 65239429404585136634285305535322032323436768900116370
Received MACc: 36168986042308736078813116828113239432942105781140847
MAC check is equal. Secure connection established.
NOTE: Enter 'quit' to end the program.
WAITING...
Received:
pk.message 'Ks(m)' = 107138202181152174215
pk.signature 'Ks(Ka-(H(m)))' = 0
pk.sessionKey 'Kb+(Ks)' = 2134474909
Message is authentic
Decrypted Result: Hello!
RECEIVED: Hello!
Project 3 - Client (run) running... (1 more...)
563:1 INS
Type here to search
9:34 PM
11/27/2018


Project 3 - Client - NetBeans IDE 8.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Search (Ctrl+I)
<default config>
Output
Project 3 - Server (run)
Project 3 - Client (run)
Ciphers: [1, 3, 4, 5]
Received: 2134474909;3606558803413074140765708483036072434255614808026234696265860502813584511691356280636039642619945930543971584611966053624679782676859390850934919957027294778482302569445984063543916 3
PMS: 549277779
Product: 38897193962566338929821 6830
Kc: 194485969812831694649108415
Mc: 378247924540376811961832939807996915295517544238122 25
Ks: 756495849080753623923665879615993830591035088476244 50
Ms: 756495849080753623923665879615993830591035088476245 29
MACc: 361689860423087360788131168281132394329421057811408 47
MACs: 652394294045851366342853055353220323234367689001163 70
Received MACc: 361689860423087360788131168281132394329421057811408 47
MAC check is equal. Secure connection established.
NOTE: Enter 'quit' to end the program.
WAITING...
Received:
pk.message 'Ks(m)' = 107138202181152174215
pk.signature 'Ks(Ka-(H(m)))' = 0
pk.sessionKey 'Kb+(Ks)' = 2134474909
Message is authentic
Decrypted Result: Hello!
RECEIVED: Hello!
SEND: Good Morning. How are you?
WAITING...
Received:
pk.message 'Ks(m)' = 215139133170153223169128209139174145105160167151119215146227
pk.signature 'Ks(Ka-(H(m)))' = 0
pk.sessionKey 'Kb+(Ks)' = 2134474909
Message is authentic
Decrypted Result: I am swell, thanks!
RECEIVED: I am swell, thanks!
SEND:
Project 3 - Client (run) running... (1 more...)
563:1 INS
Type here to search
9:34 PM
11/27/2018