Question table:

|  |  |
| --- | --- |
| Id of Client: | 0001 |
| Id of Server: | 0010 |
| Id of KDC: | 0011 |
| Id of TGS: | 0100 |
| KC:  **(if student no. s3701234)** | F3711351F3711351F3711351F3711351F3711351F3711351F3711351F3711351 |
| KTGS:  **(if student no. s3701234)** | 1351F3711351F3711351F3711351F3711351F3711351F3711351F3711351F371 |
| KS:  **(if student no. s3701234)** | 3711351F3711351F3711351F3711351F3711351F3711351F3711351F3711351F |
| Session key KC,TGS: | 0123456712345678234567893456789a0123456712345678234567893456789a |
| Session key KC,S: | a9876543987654328765432176543210a9876543987654328765432176543210 |
| Ticket TC,TGS = {KC,TGS, C}: | 0123456712345678234567893456789a0123456712345678234567893456789a0001 |
| Ticket TC,S = {KC,S, C}: | a9876543987654328765432176543210a98765439876543287654321765432100001 |
| Session key sk: | 0123456701234567012345670123456701234567012345670123456701234567 |
| Timestamp ts: | 1536755037 |
|  | |
| **Tag ①: Client sends a request to the KDC for a “ticket-granting ticket” (TGT)** | |
| Number of phase: | Phase 1 |
| Message transferred: | Plaintext {C, TGS} |
| Value of transferred message: | {00010011} |
| **Tag ②: KDC responds to client** | |
| Number of phase: | Phase 1 |
| Message transferred: | {KC,TGS, TGS}KC= {0123456712345678234567893456789a0123456712345678234567893456789a0100}KC  ,  {TC,TGS}KTGS={KC,TGS, C}KTGS ={0123456712345678234567893456789a0123456712345678234567893456789a0001 }KTGS |
| Value of transferred message: | {wRFRqEnUIxUoOoXVuVCDFWBj+K3G2z1pFTUASLAhDgJ9rol2se3bfDro5IOZ9ldK4JyEBwPn4OKT/y5YWTa9KxRNPrOaICK95DyRZwEzByo=}, {wWl7M2KpZdgbG1rFbq9Bv+5FMIdNNcTYGxGYFuWvJbs33uYwdWqnlGOsrXIL1dD59sU/TceRkZq2NHqZhUZYHp9O7efauLttKYn4rlYZgG0=} |
| **Tag ③: Client requests a ticket to communicate with server from the ticket-granting service (TGS)** | |
| Number of phase: | Phase 2 |
| Message transferred: | {ts…}KC,TGS = {1536755037} KC,TGS,  {TC,TGS}KTGS = {0123456712345678234567893456789a0123456712345678234567893456789a0001} KTGS,  S = 0010 |
| Value of transferred message: | {LtepvYiUPEeT3TNRJyNfBw== },  {wWl7M2KpZdgbG1rFbq9Bv+5FMIdNNcTYGxGYFuWvJbs33uYwdWqnlGOsrXIL1dD59sU/TceRkZq2NHqZhUZYHp9O7efauLttKYn4rlYZgG0=},  0010 |
| **Tag ④: TGS returns a ticket for client to talk to server** | |
| Number of phase: | Phase 2 |
| Message transferred: | {KC,S, S}KC,TGS = {a9876543987654328765432176543210a98765439876543287654321765432100010}KC,TGS,  {TC,S}KS = {a9876543987654328765432176543210a98765439876543287654321765432100001}KS |
| Value of transferred message: | {oDPp3AW48JJPiC3l+pj8ghw2lMw7AYf2fTwRIylQV6SwEUoawNdxOZlL05E9R5p75shYG+nyp2b3pz3ZPDEV4qECZKDENeA8U8kA66oDX5M= },  {oWjdNavjjw3bcDCjHpfJY1I/nnUkQq4hRDCronkQkX83X9DMF0UKpOOsfEy4hSFcMGMBGx0JySKtJQn4CmDNZyw74hplUKNZTiP2ngDDMh8= } |
| **Tag ⑤: Client sends the ticket to server along with an authenticator to establish a shared secret** | |
| Number of phase: | Phase 3 |
| Message transferred: | {C, ts, sk}KC,S = {000115367550370123456701234567012345670123456701234567012345670123456701234567}KC,S,  {TC,S}KS = {KC,S, C}KS = {a9876543987654328765432176543210a98765439876543287654321765432100001}KS, |
| Value of transferred message: | {YHmjr3W8r/rtIqv5oXKHKKG0/cWY33UoM9b2op3bGfvBeMqbfjYJehgunJhYLCVhPOJ91Id1iHoMY37PL80u/wZYNwvHcRqYD8lgIskPyDA=},  {oWjdNavjjw3bcDCjHpfJY1I/nnUkQq4hRDCronkQkX83X9DMF0UKpOOsfEy4hSFcMGMBGx0JySKtJQn4CmDNZyw74hplUKNZTiP2ngDDMh8= } |
| T**ag ⑥: Server decrypts the ticket to obtain the KC,S and replies to client with proof of possession of the shared secret** | |
| Number of phase: | Phase 3 |
| Message transferred: | {ts, sk}KC,S = {15367550370123456701234567012345670123456701234567012345670123456701234567}KC,S |
| Value of transferred message: | {LZJovBDQvTRVmvpRRyCT1pXJDSJcvm3IExaRXGph6aGasTjEGt++OkXwXD4J5NwWyuFMG0ASr3Fl6tOkymhmzZtnRn0zoZTU3o6XeCEURXY=} |