# INTE2401/2402 Lab 8

Student ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This week’s lab concentrates on establishing secure communication between two parties. We utilise online AES-CBC tool to demonstrate the model of Kerberos network authentication protocol. Online AES encryption and decryption: <http://rubbingalcoholic.github.io/cowcrypt/demos/aes.html>

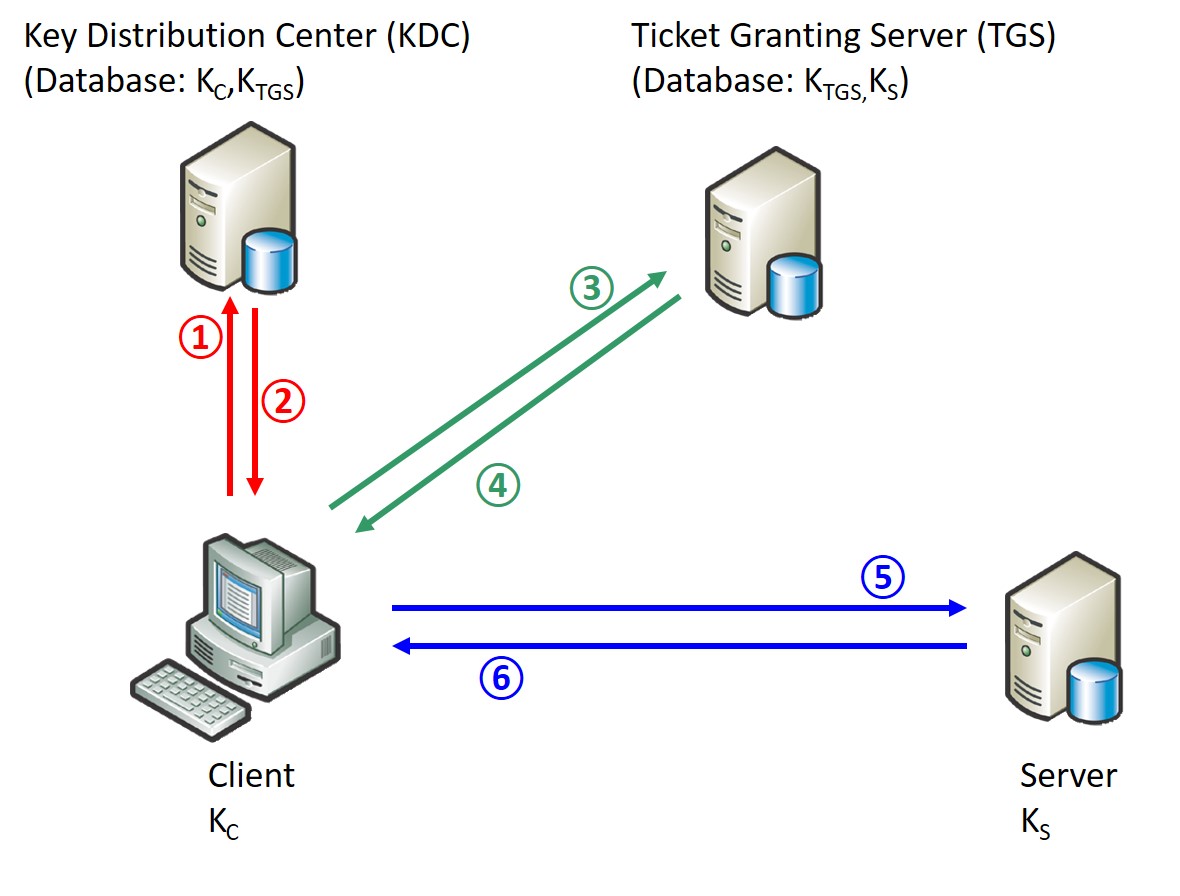


Figure 1. Model of Kerberos protocol

In this task, we demonstrate how authentication being provided in each phase. For brevity, we omit the “Lt” and “nC” in all phases. We use online AES-CBC tool to perform encryption. Noted that the encryption of multiple messages is performed over the **concatenation** of all messages. For example, {KC,TGS, TGS}KC is performed in the way {KC,TGS || TGS}KC. Besides, all secret keys are derived from the last 4 digits of your **student no**, and **replace the ‘s’ in student no with ‘F’**. Other required informations and example are provided in the table below. Noted that the encryption of multiple Task is emulated by filling the question table.

Question table:

|  |  |
| --- | --- |
| Id of Client: | 0001 |
| Id of Server: | 0010 |
| Id of KDC: | 0011 |
| Id of TGS: | 0100 |
| KC:  **(if student no. s3710646)** | F3710646F3710646F3710646F3710646F3710646F3710646F3710646F3710646 |
| KTGS:  **(if student no. s3710646)** | 0646F3710646F3710646F3710646F3710646F3710646F3710646F3710646F371 |
| KS:  **(if student no. s3710646)** | 6460173F6460173F6460173F6460173F6460173F6460173F6460173F6460173F |
| 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:  **(Example)** | Phase 1 |
| Message transferred:  **(Example)** | Plaintext {C, TGS} |
| Value of transferred message:  **(Example)** | {00010011} |
| **Tag ②: KDC responds to client** | |
| Number of phase: | Phase 1 |
| Message transferred:  **(Example)** | {KC,TGS, TGS}KC= {0123456712345678234567893456789a0123456712345678234567893456789a0100}KC  ,  {TC,TGS}KTGS={KC,TGS, C}KTGS ={0123456712345678234567893456789a0123456712345678234567893456789a0001 }KTGS |
| Value of transferred message:  **(Example)** | {dGrQp71w0D/oUjEStSs02eBMPv9t04e9vuNS2L/El4+E7FHYCmPdSoZBlRn+vnWWK7rhTxbKkklSTiHprJU542JXWemm36t32o3Jq8NsD04=}  {XCQZbepTqfuzx68MYlW2OK836urBY88p0JGuLbeSbtszaOxAeGG8MCofzs9cudZe/HlY+LLRTGqaRmRkQHdNZbcJpS+dPCTmo+IRYUkfpvM=} |
| **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 |
| Value of transferred message: | {LtepvYiUPEeT3TNRJyNfBw== }  {XCQZbepTqfuzx68MYlW2OK836urBY88p0JGuLbeSbtszaOxAeGG8MCofzs9cudZe/HlY+LLRTGqaRmRkQHdNZbcJpS+dPCTmo+IRYUkfpvM=} |
| **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=}  {8IOO7myCT9BzOZybQQGXUJ6Q5zegZNY5PVyxO8tKnKDBVckxhbtsTRW9MCvGeeM7JzWn2d4nZJfxVol1bPUBVNhyWDrbiDNXHmu80PVCjdA= } |
| **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={ a9876543987654328765432176543210a98765439876543287654321765432100001}KS |
| Value of transferred message: | { YHmjr3W8r/rtIqv5oXKHKKG0/cWY33UoM9b2op3bGfvBeMqbfjYJehgunJhYLCVhPOJ91Id1iHoMY37PL80u/wZYNwvHcRqYD8lgIskPyDA=}  {8IOO7myCT9BzOZybQQGXUJ6Q5zegZNY5PVyxO8tKnKDBVckxhbtsTRW9MCvGeeM7JzWn2d4nZJfxVol1bPUBVNhyWDrbiDNXHmu80PVCjdA=} |
| 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=} |