CMSC 426
Principles of Computer Security

Lecture 17

Kerberos and Exam Review

Last Class We Covered

- Linux authentication

- Windows authentication
  - Standalone system authentication
  - Domain authentication

Any Questions from Last Time?

Today's Topics

- Kerberos protocol

- Exam Review

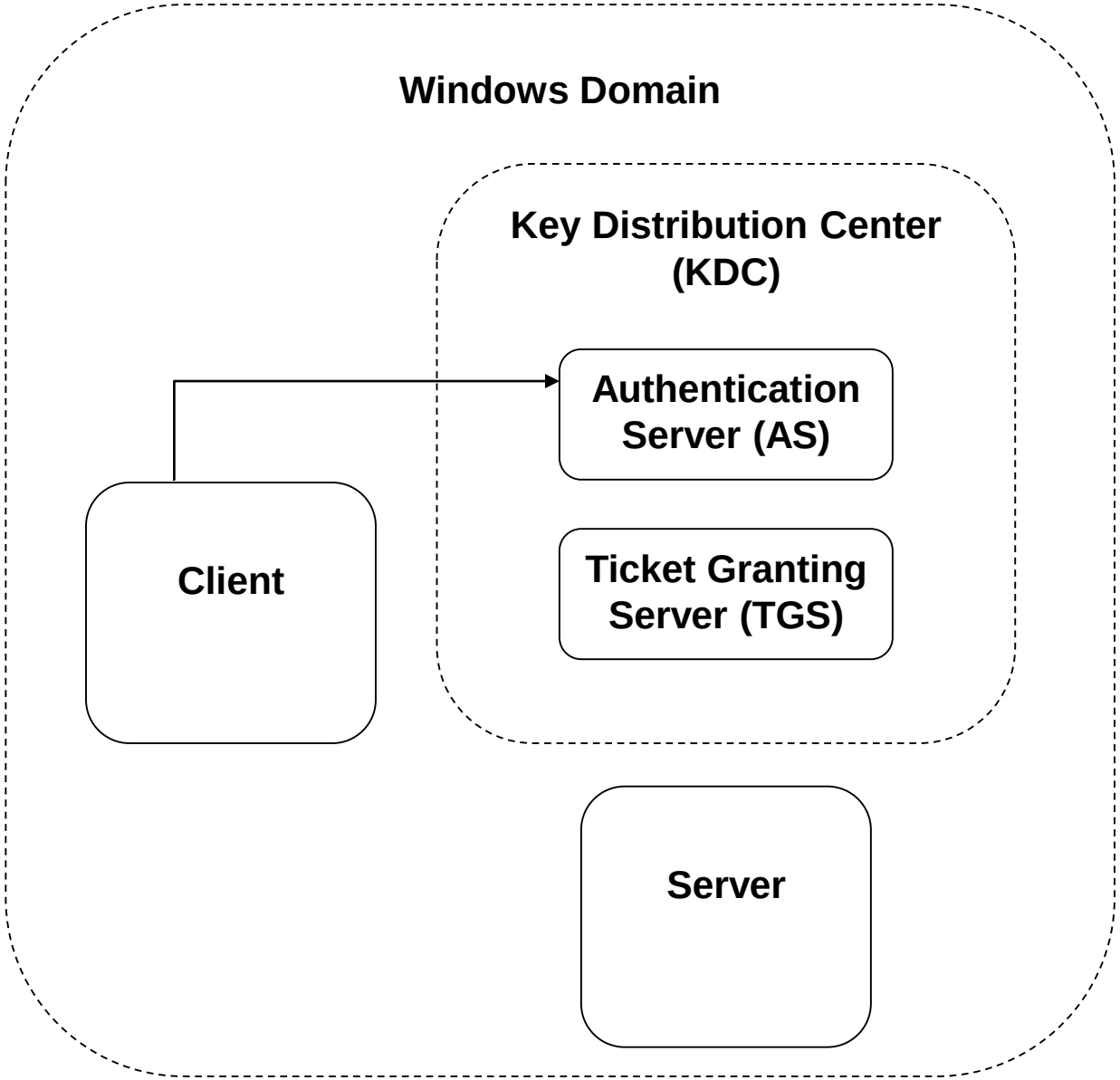
Kerberos Protocol

Kerberos Protocol

- Leading standard protocol for remote authentication
  - Used by many OSes, not just Windows
  - Will mostly be talking about it in the context of Windows domains
- Manages client-server interactions using a Key Distribution Center (KDC)
- Key Distribution Center provides two services:
  - Authentication Service (AS)
  - Ticket-Granting Service (TGS)

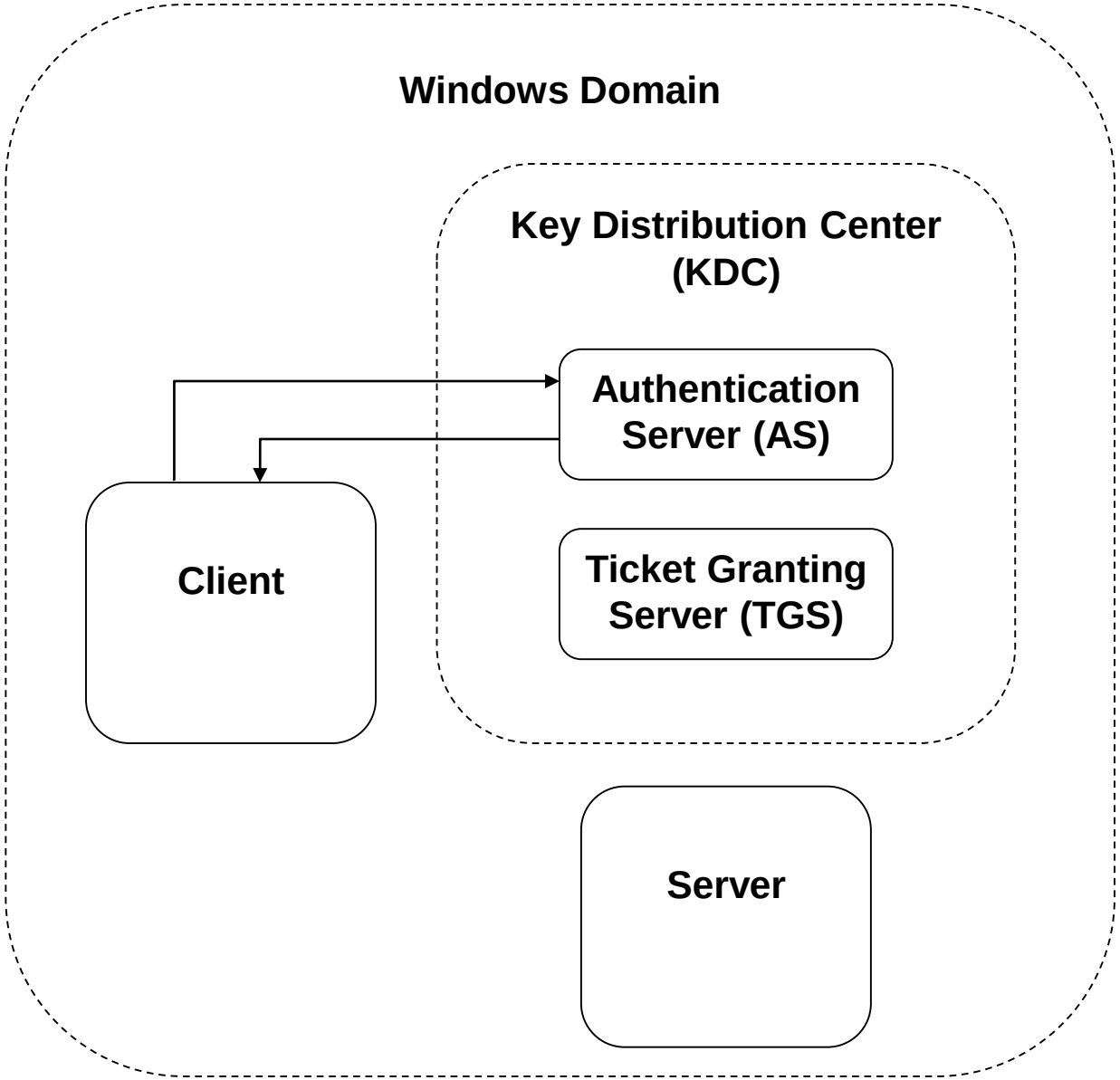
Kerberos Protocol

- Each time the client logs into a domain, they send their user ID and request for a Ticket-Granting Ticket (TGT) to the AS



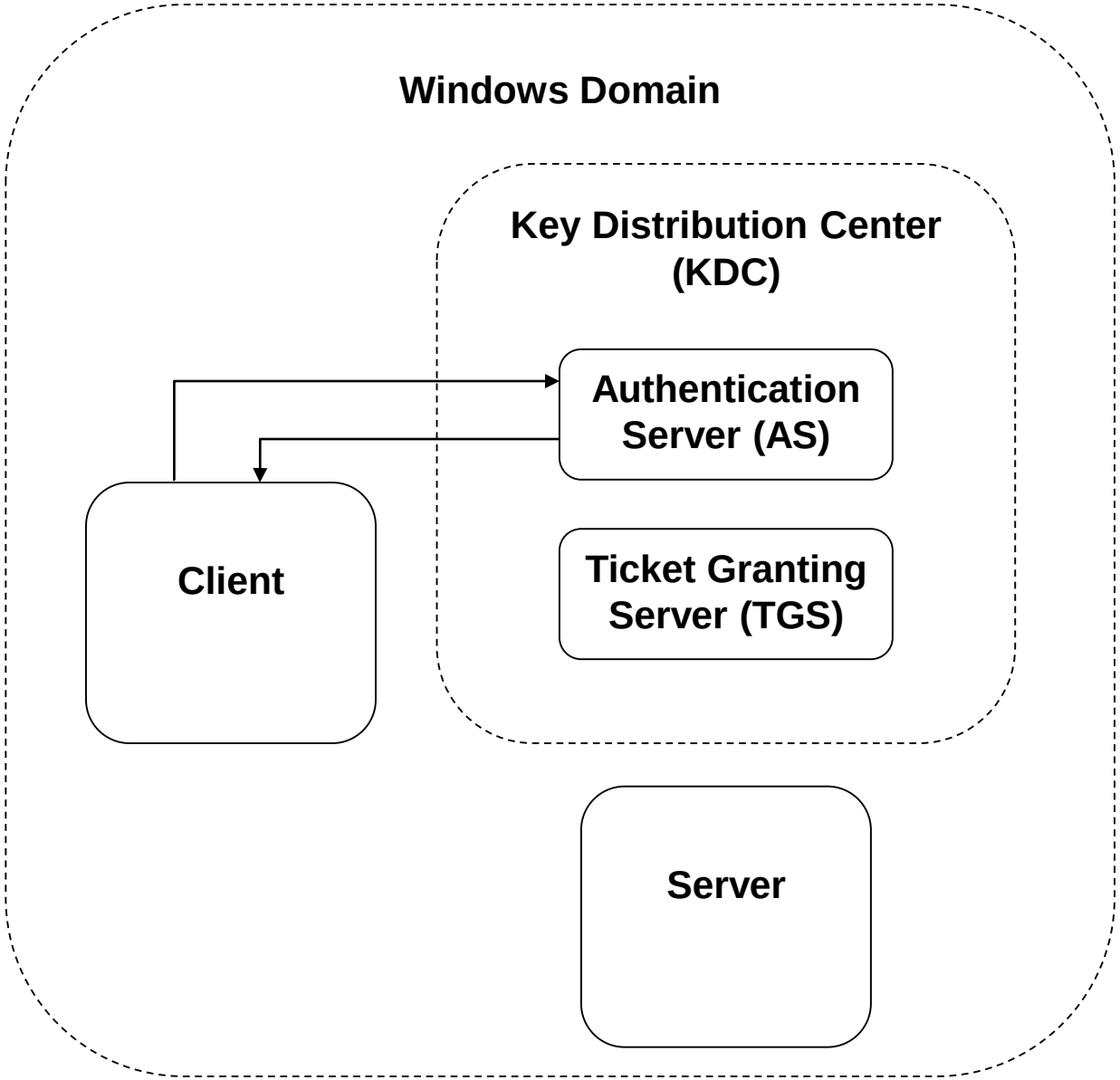
Kerberos Protocol

- The AS responds with two messages:
  - The TGT, which contains the user's ID, TGS ID, timestamp, IP address, lifetime, and *TGS session key*, encrypted using the TGS secret key
  - The TGS ID, timestamp, lifetime, and *TGS session key*, encrypted using the client's password hash as a key



Kerberos Protocol

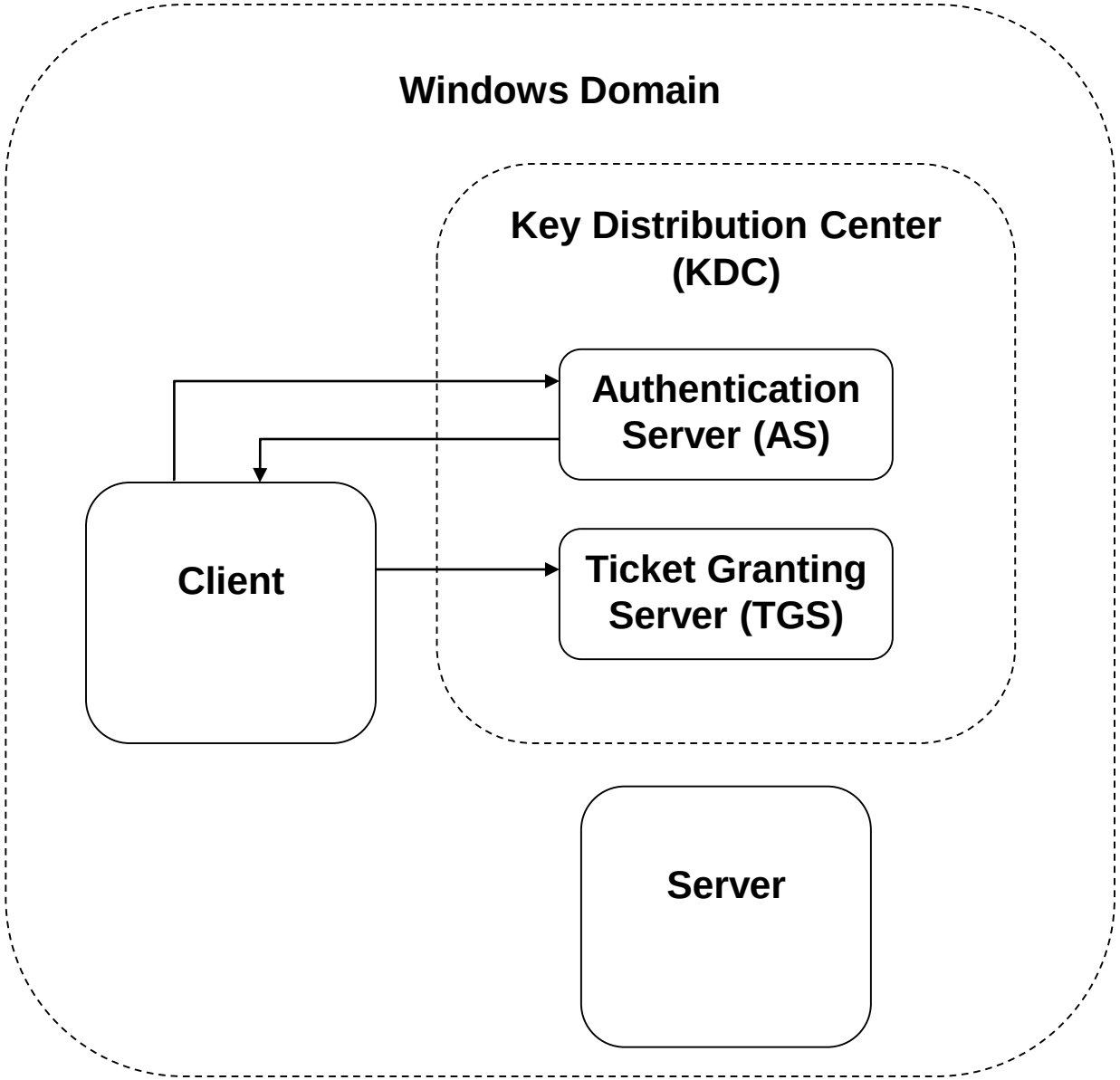
- The user enters their password and decrypts the second message
- The client prepares an *Authenticator*, which contains their user ID and timestamp, and encrypts it using the TGS session key



Kerberos Protocol

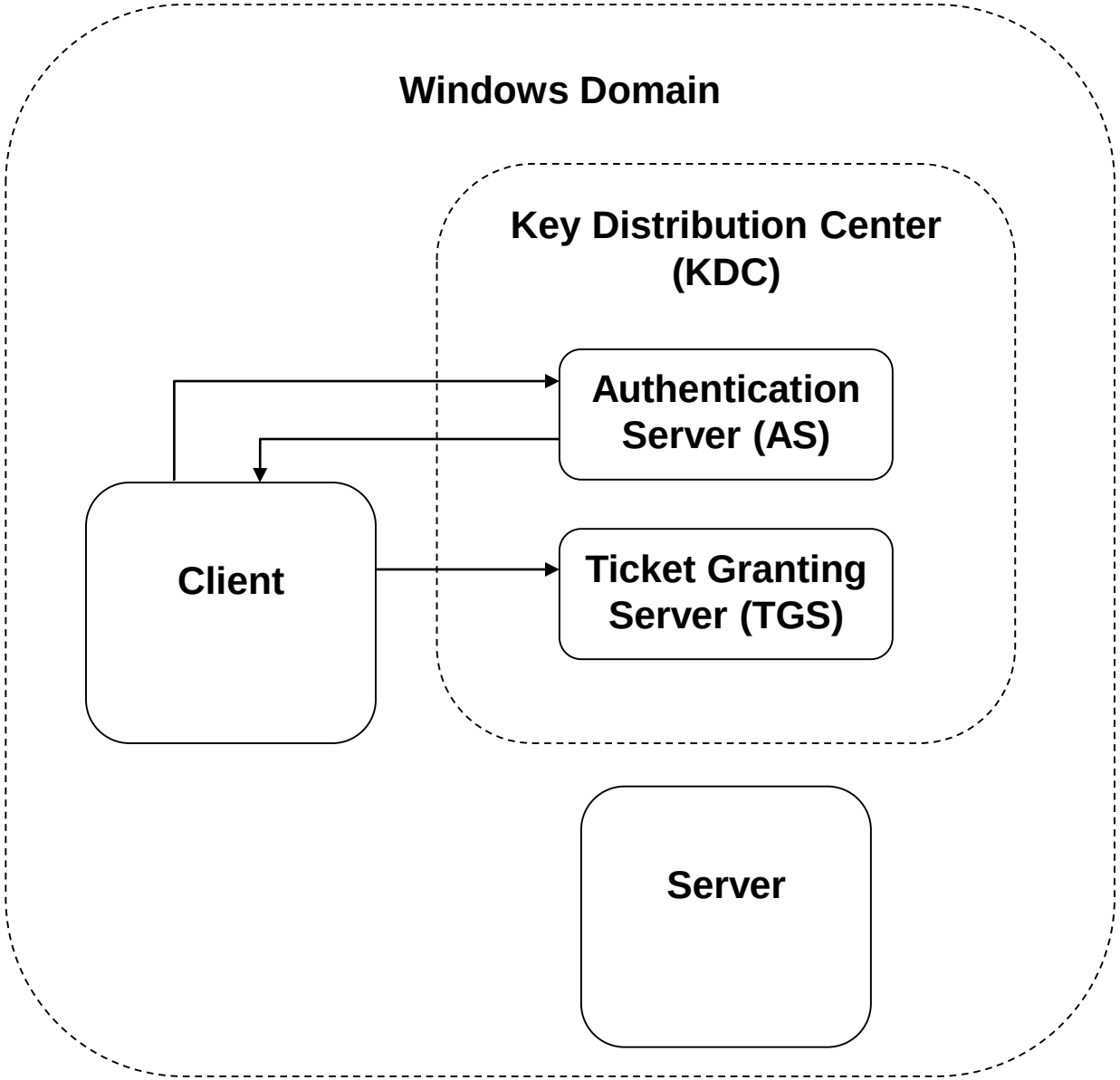
- Any time the client needs to communicate with a server, it sends a message to the TGS requesting a ticket to the server

- The client also sends the encrypted TGT and encrypted Authenticator to the TGS



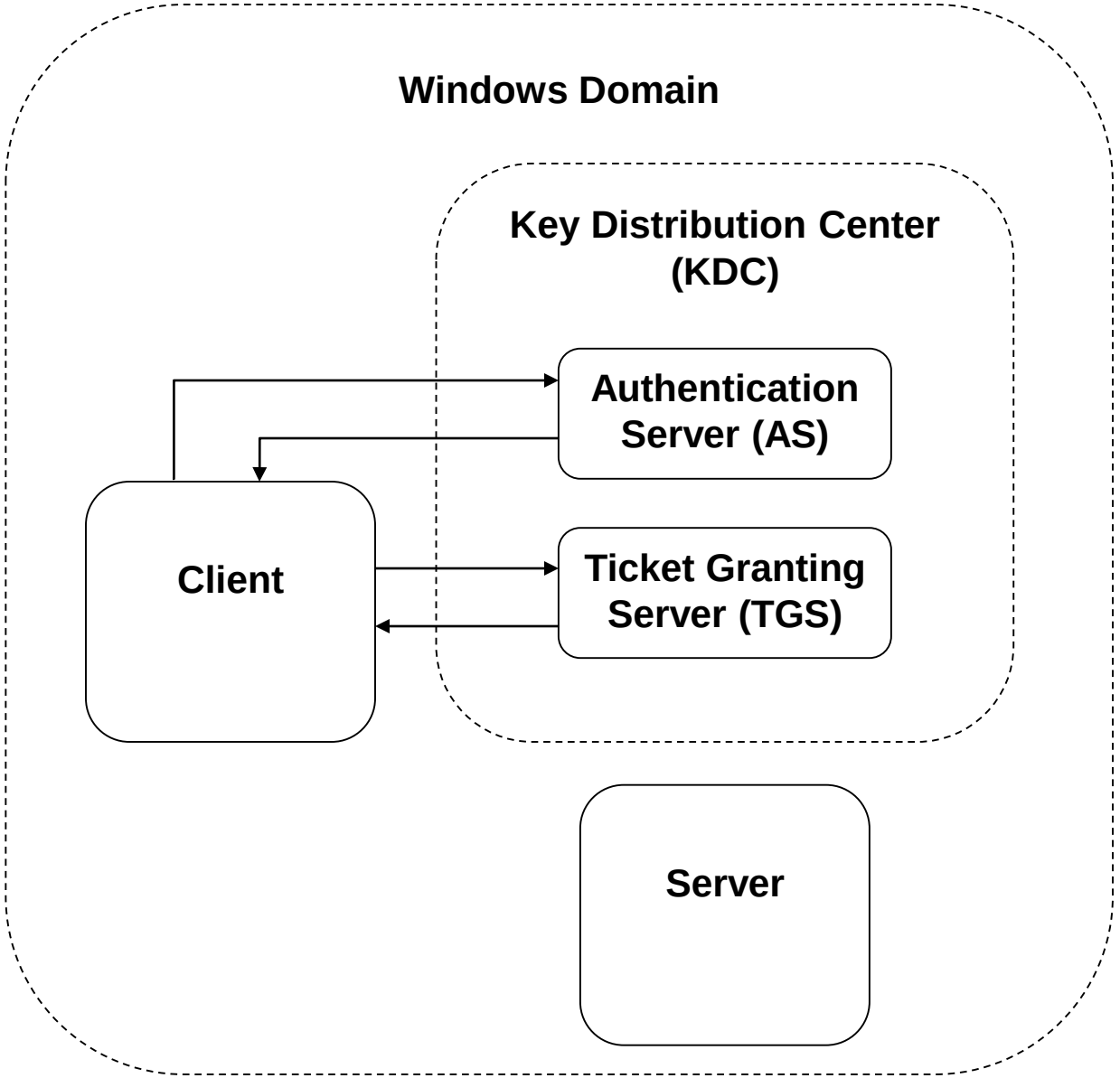
Kerberos Protocol

- The TGS decrypts the TGT with its secret key
- The decrypted TGT contains the *TGS session key*, which the TGS uses to decrypt the Authenticator
- The TGS validates all information



Kerberos Protocol

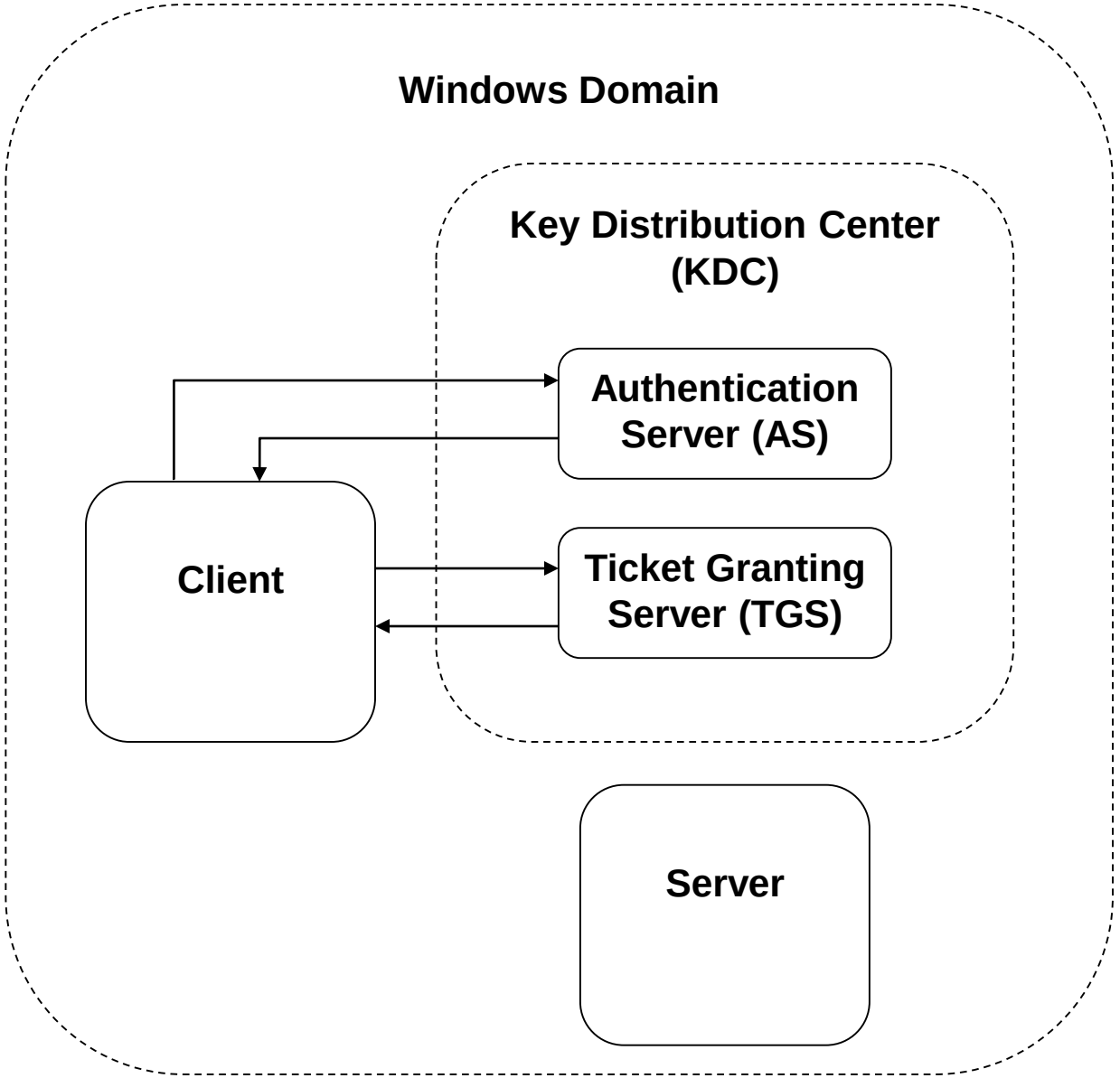
- The TGS sends two messages to the client:
  - A service ticket that contains the user's ID, the service's ID, IP address, timestamp, lifetime, and *service session key*, all encrypted using the service secret key
  - The service's ID, timestamp, lifetime, and *service session key*, encrypted using the TGS session key



Kerberos Protocol

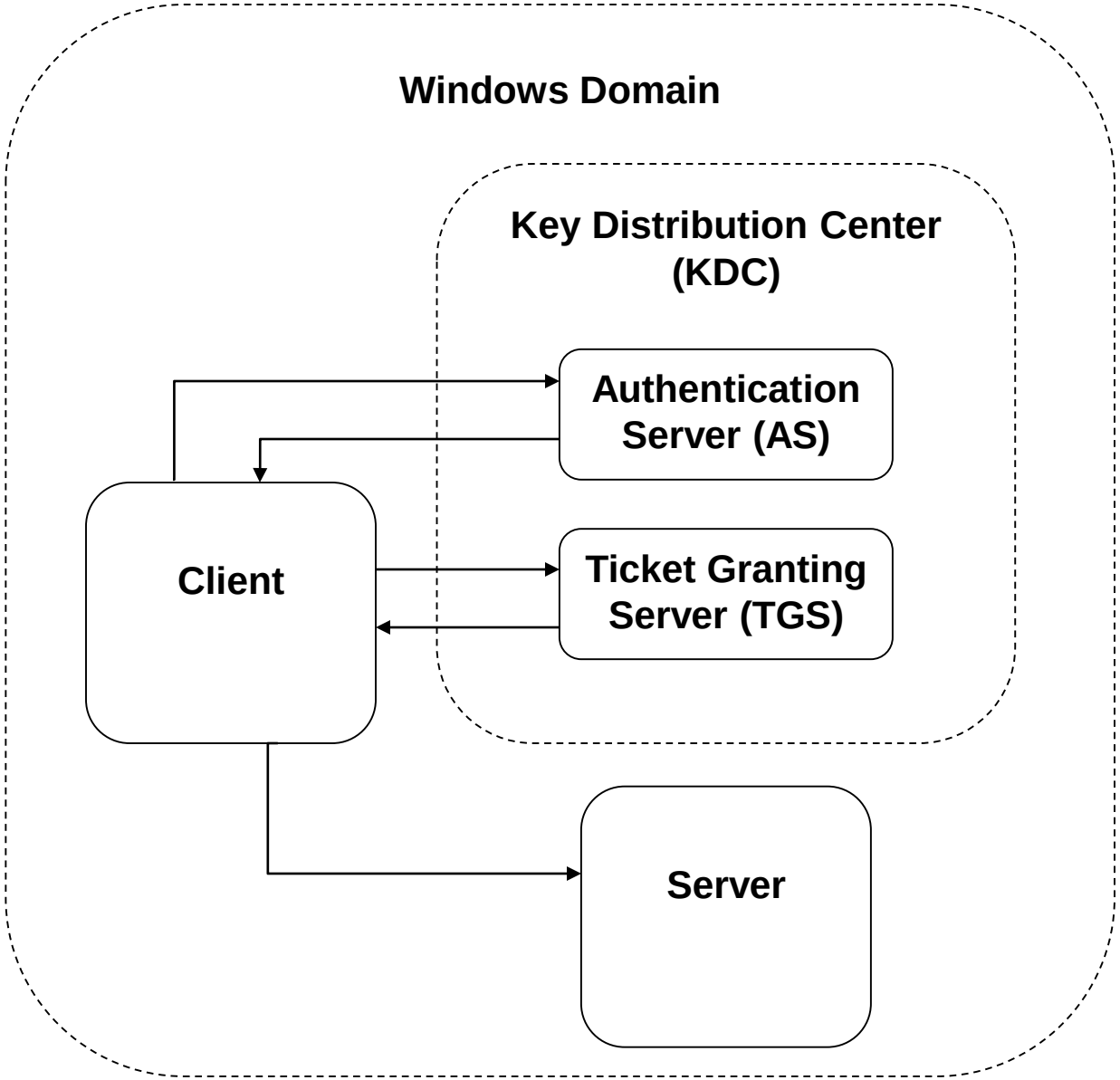
- The client decrypts the second message using the TGS session key

- The client prepares a ***second*** *Authenticator* that contains the user's ID and timestamp and is encrypted using the service session key



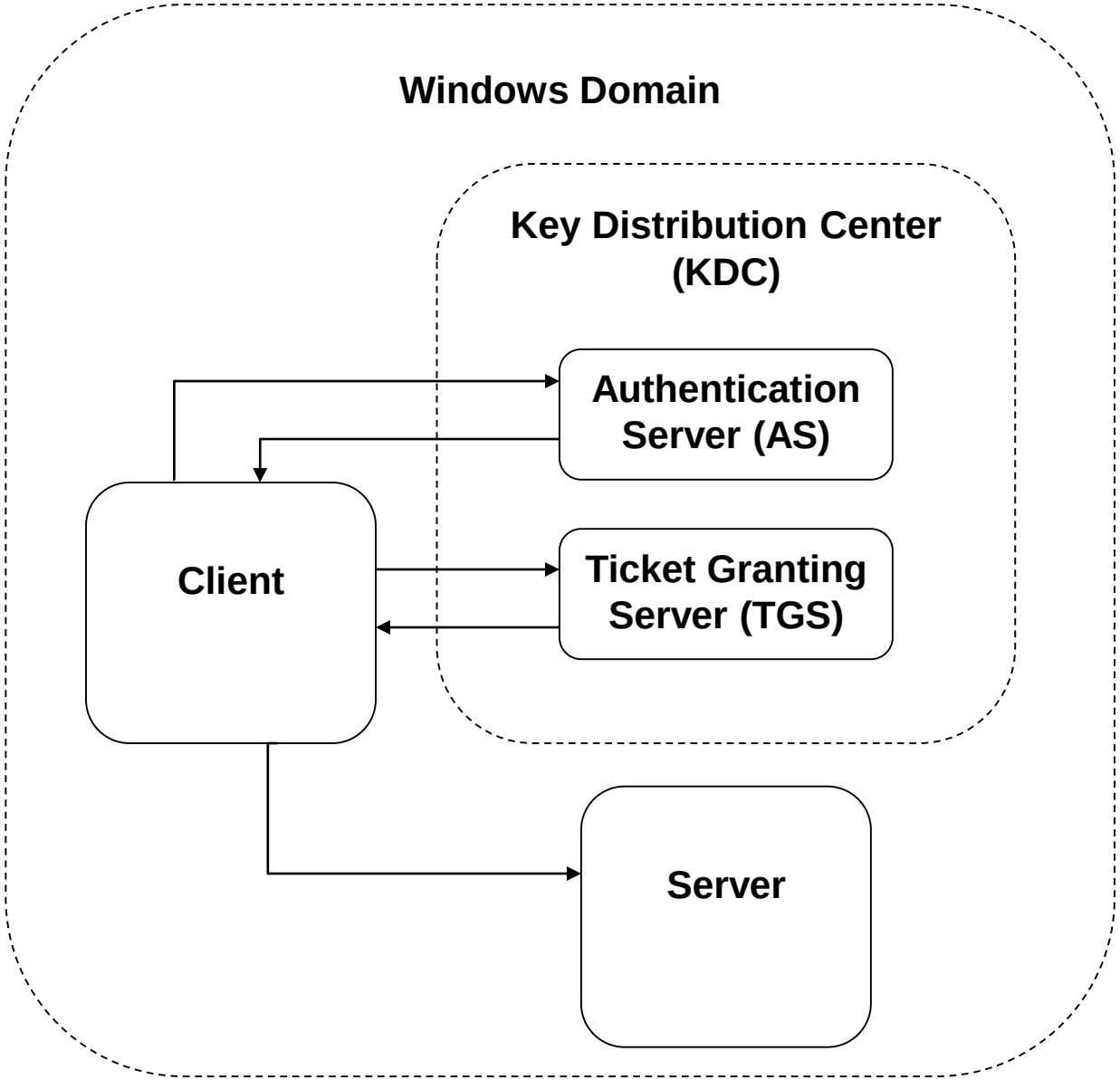
Kerberos Protocol

- The client sends the service ticket and the second Authenticator to the server



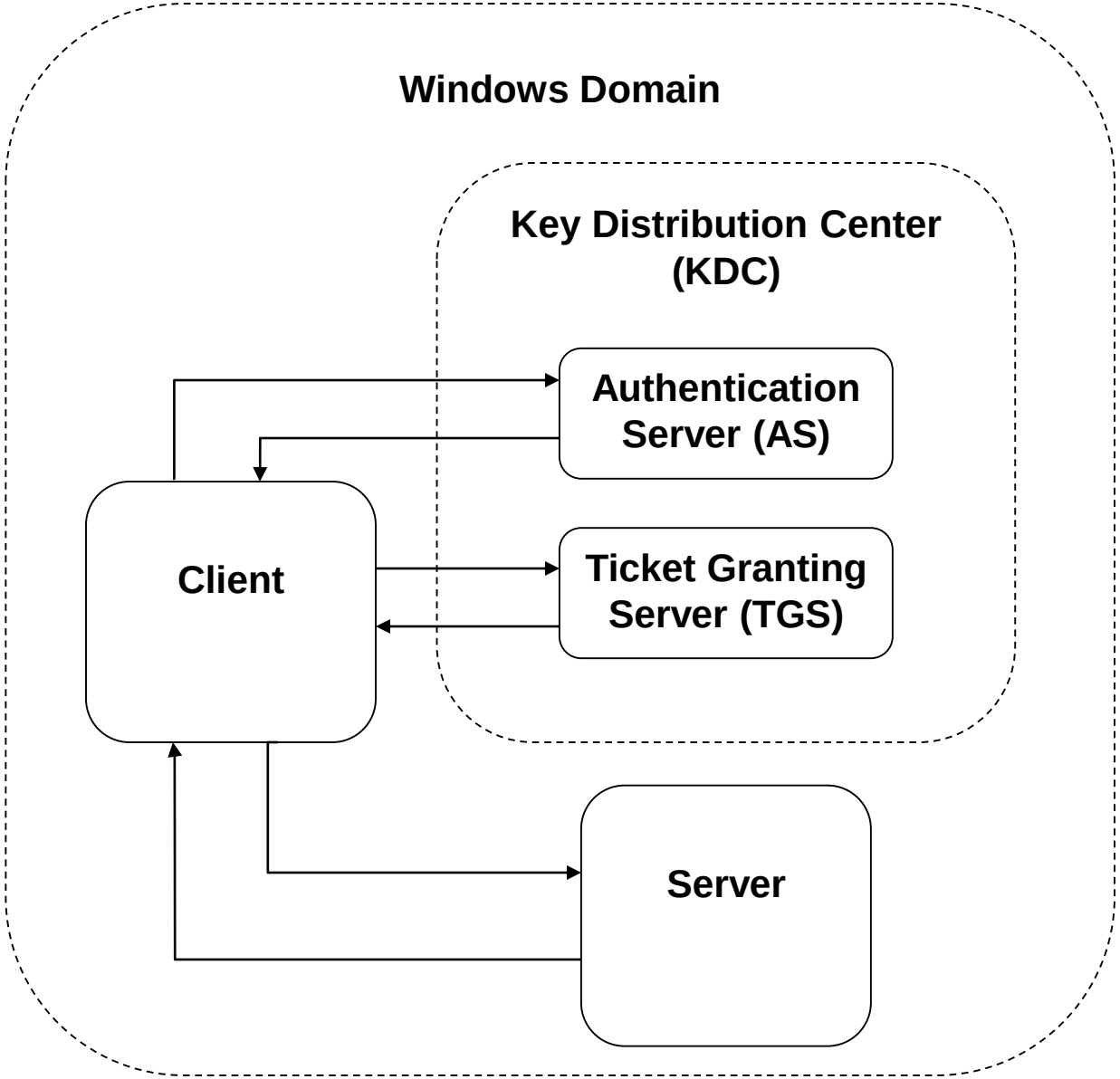
Kerberos Protocol

- The server uses its secret key to decrypt the service ticket, which includes the *service session key*
- The server decrypts the second Authenticator with the service session key
- The server validates all information



Kerberos Protocol

- The server prepares a ***third*** *Authenticator* containing the server's ID and the timestamp, and encrypts it with the service session key
- The server sends its Authenticator to the client, which decrypts it
- Authentication complete!!!



Exam Review

Topics

- Cryptography
  - DES, 3DES, AES, RSA, Diffie-Hellman
  - Block encryption, weak vs strong collision, random numbers
  - ~*~ Math ~*~
- Ethics
- Passwords
  - Hashing, attacks, dictionaries, rainbow tables, salting
  - Windows/Linux (LM, NTLM)
- Kerberos

Calculators & Formulas

- You do not need a calculator for the exam
  - Show your work, and we'll be forgiving of math-based errors

- Formulas will be given to you on the exam itself
  - They will not be labelled, and there will be bogus formulas
  - You need to be able to recognize the formulas, but do not need to memorize them
    - *e.g.*, $y = mx + b$
      $y = x^2 + C$
      $x = hop/skip$

Announcements

- Next class will be OS Security Features
  - Topic will NOT be on the upcoming exam

- Homework 2 is due tonight
- Homework 3 is out and is due Tuesday in person by 5:30

- Midterm 2 is happening on Tuesday (April 23rd)