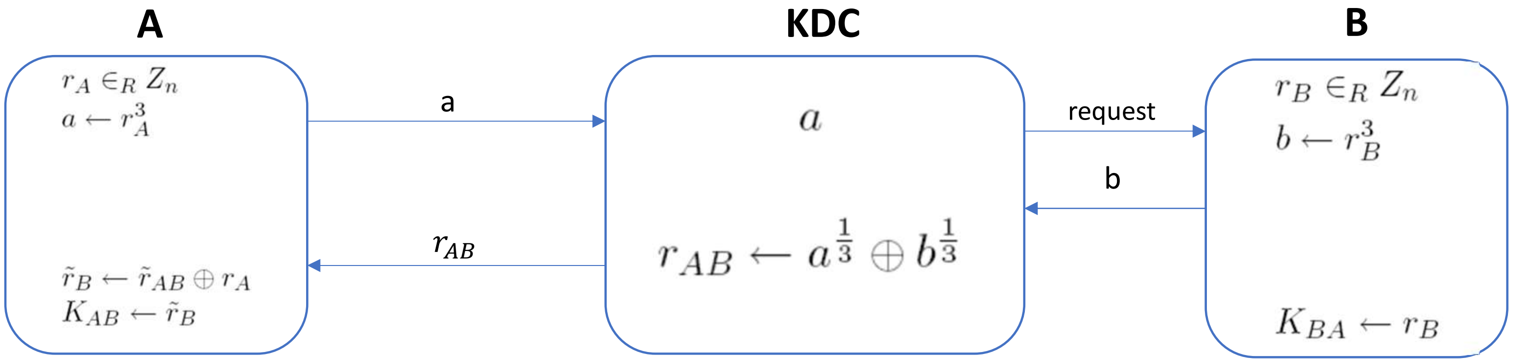
Tutorial 10

SOEN-321

TMN Key Distribution Protocol



A

$r_A \in_R Z_n$

$a \leftarrow r_A^3$

$\tilde{r}_B \leftarrow \tilde{r}_{AB} \oplus r_A$

$K_{AB} \leftarrow \tilde{r}_B$

a

r_{AB}

KDC

a

$r_{AB} \leftarrow a^{\frac{1}{3}} \oplus b^{\frac{1}{3}}$

request

b

B

$r_B \in_R Z_n$

$b \leftarrow r_B^3$

$K_{BA} \leftarrow r_B$

Based on two secure primitives:

- Information theoretic.
- computational complexity (RSA e=3).

Attacker observes:

a , b , r_{AB}

and needs to find r_b

$$r_b = a^{\frac{1}{3}} \oplus r_{AB} \quad \text{or} \quad r_b = b^{\frac{1}{3}}$$

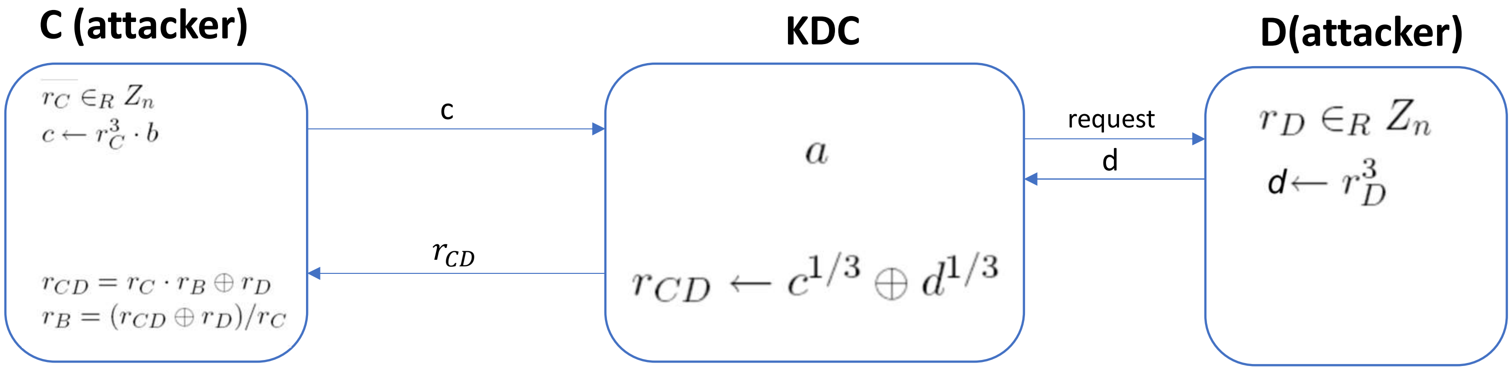
IS TMN Protocol Secure?

Based on two secure primitives:

- Not secure if collusion/cooperation of principals can happen.
- Attacker can take on the role of several principals (she will act as two principals).

- Hint for the attack:
  - KDC is a decryption service.
  - KDC input can be from a previous observed run.

TMN Key Distribution Protocol



C (attacker)

$r_C \in_R Z_n$

$c \leftarrow r_C^3 \cdot b$

$r_{CD} = r_C \cdot r_B \oplus r_D$

$r_B = (r_{CD} \oplus r_D)/r_C$

c

r_{CD}

KDC

a

$r_{CD} \leftarrow c^{1/3} \oplus d^{1/3}$

request

d

D(attacker)

$r_D \in_R Z_n$

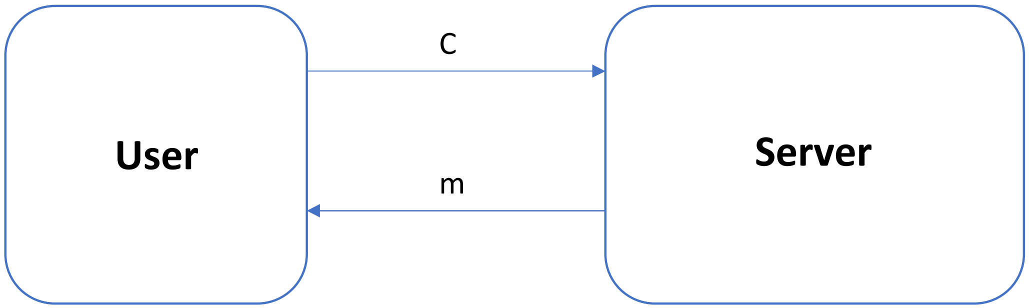
d$\leftarrow r_D^3$

- Both C and D are the attacker.
- The goal is to find r_b (from a previous observed run).

- Attacker use the following equation to find r_b (Note that attacker knows r_D *and* r_C)
- $r_{CD} = r_C \times r_B \oplus r_D$

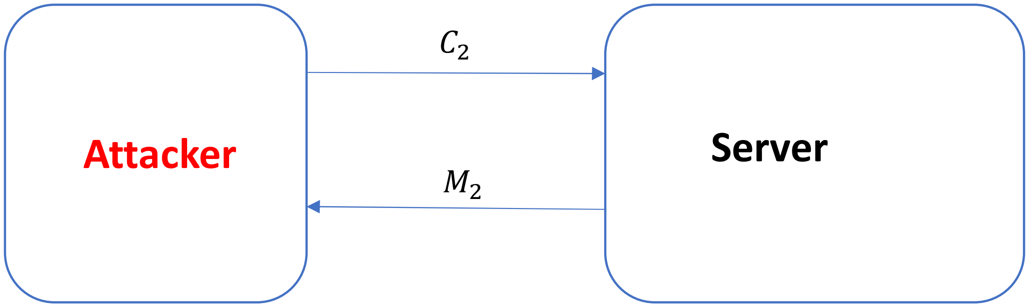
$$r_B = \frac{(r_{CD} \oplus r_D)}{r_C}$$

Chosen ciphertext attack on RSA



User sends ciphertext to the server that decrypts it and sends back the message
Server doesn’t decrypt the same ciphertext twice
Can an attacker finds the corresponding m without having the private key?

Chosen ciphertext attack on RSA



- The attacker can win the game by sending: $C_2 = C \times R^e \, mod \, n$
  (R is random number chosen by the attacker)
- Server replies with:

$$M_2 = (C \times R^e)^d = m \times R$$

- Since the attacker knows R, he finds m:

$$m = m \times R \times R^{-1}$$

- Therefore, the attacker wins the game without knowing the private key of the user.