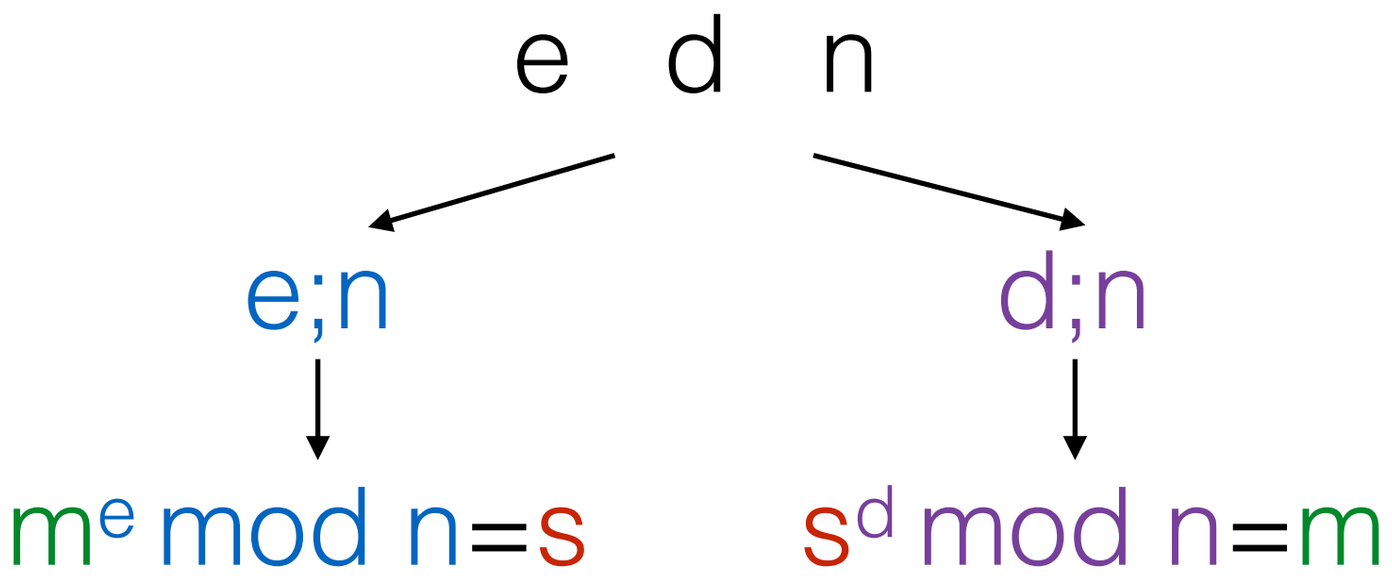
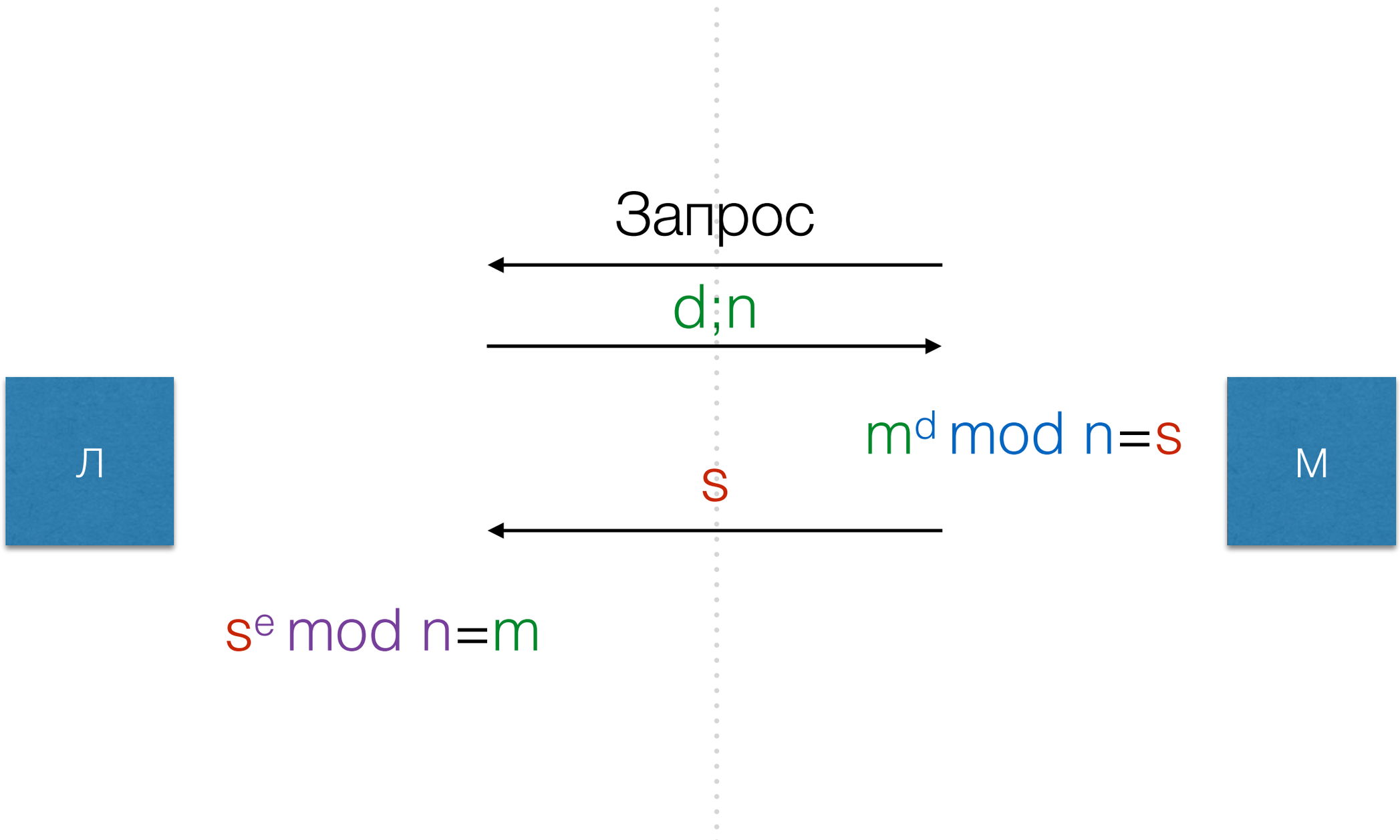
RSA

ЭЦП, Сертификаты, Мандаты

RSA



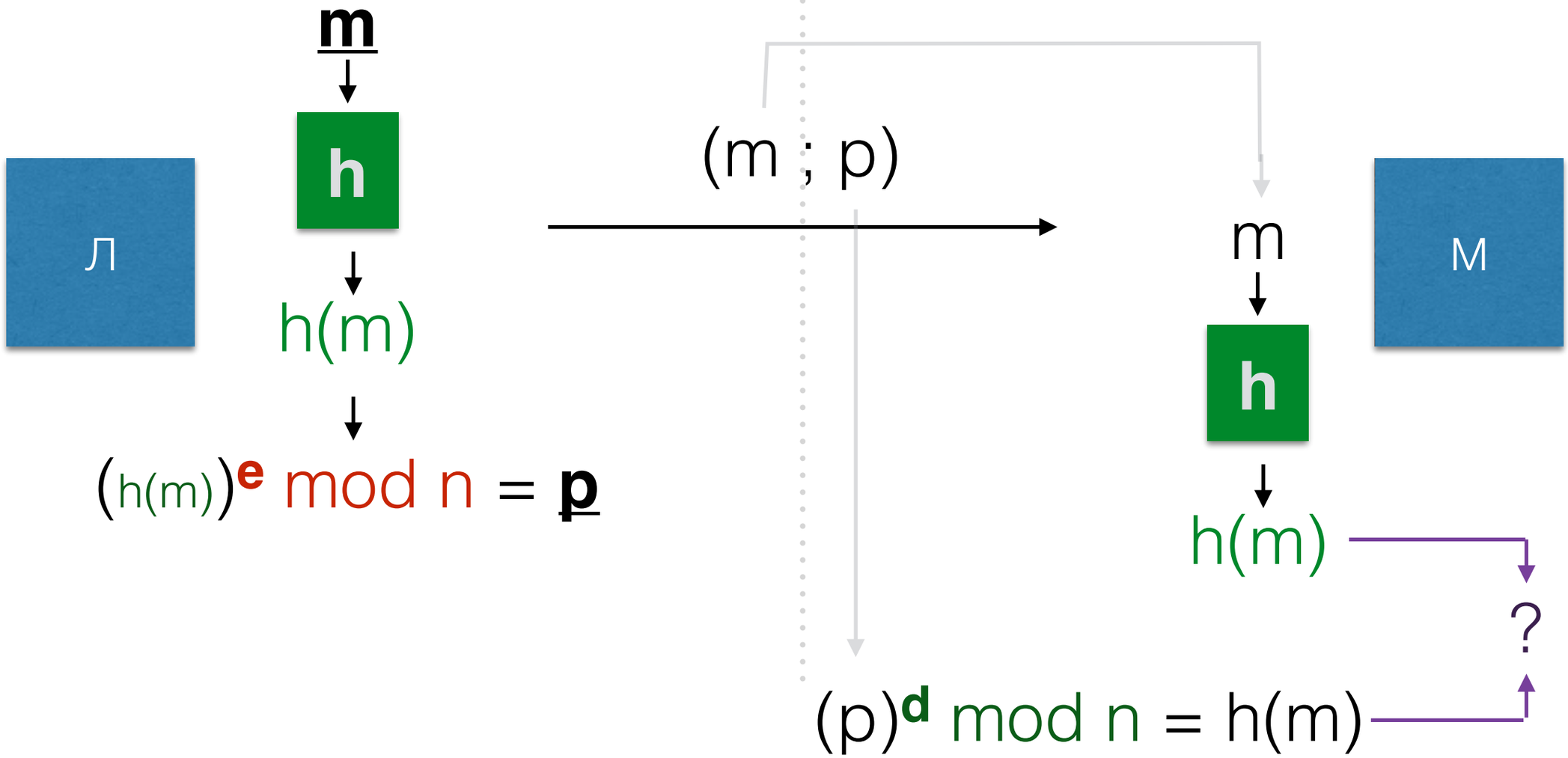
RSA



RSA

- Передача чувствительных к компрометации данных без закрытого канала
- Передача сеансового ключа для симметричного шифрования

ЭЦП



ЭЦП

- Подтверждение подлинности отправителя
- Подтверждение подлинности документа
- Подтверждает факт отсылки сообщения

ЭЦП

- Приравнена законом к личной подписи

- Позволяет реализовать сложные схемы с раздельной доставкой документа и подписи

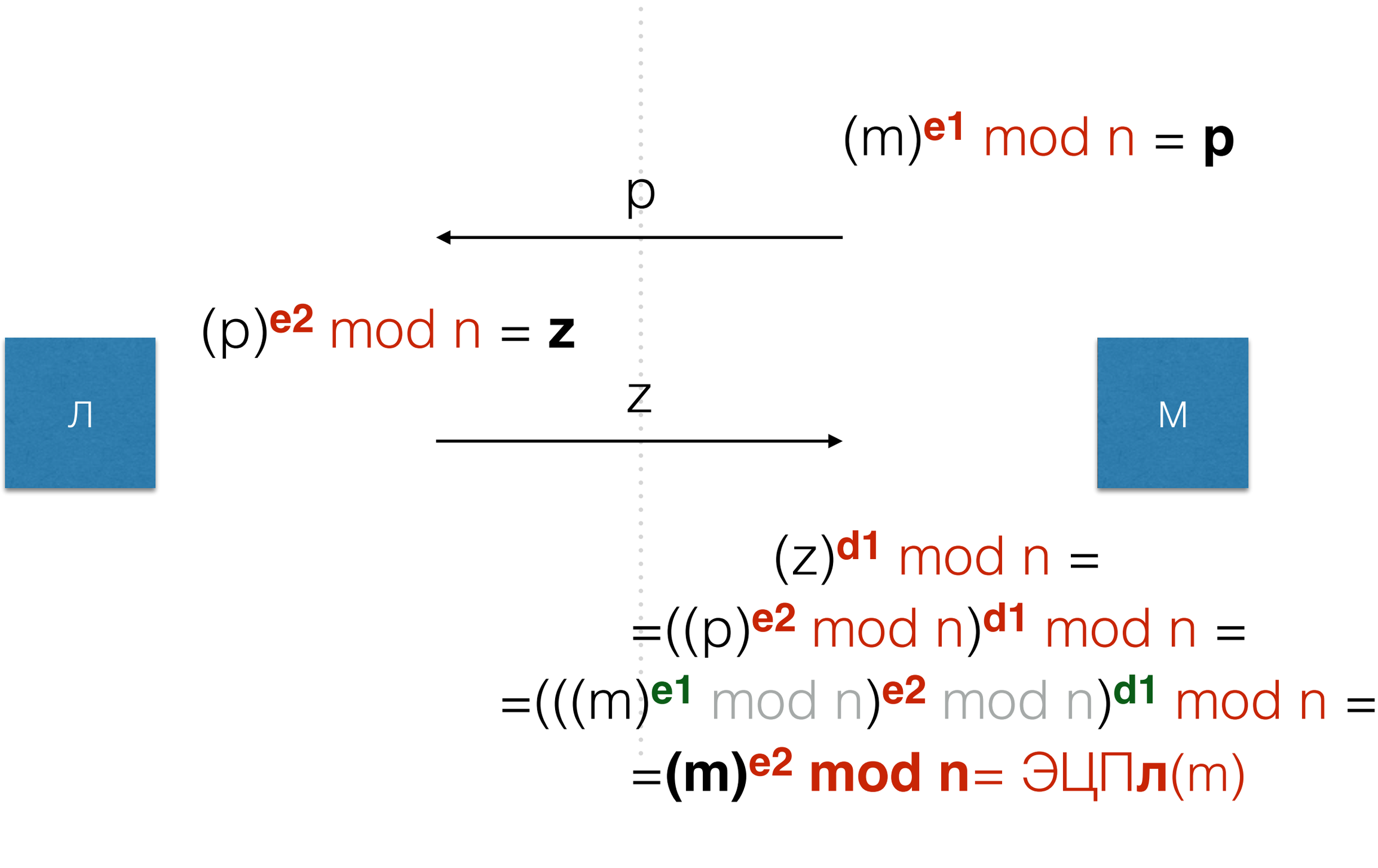
Слепая ЭЦП

или как заставить банк подписать неизвестный документ

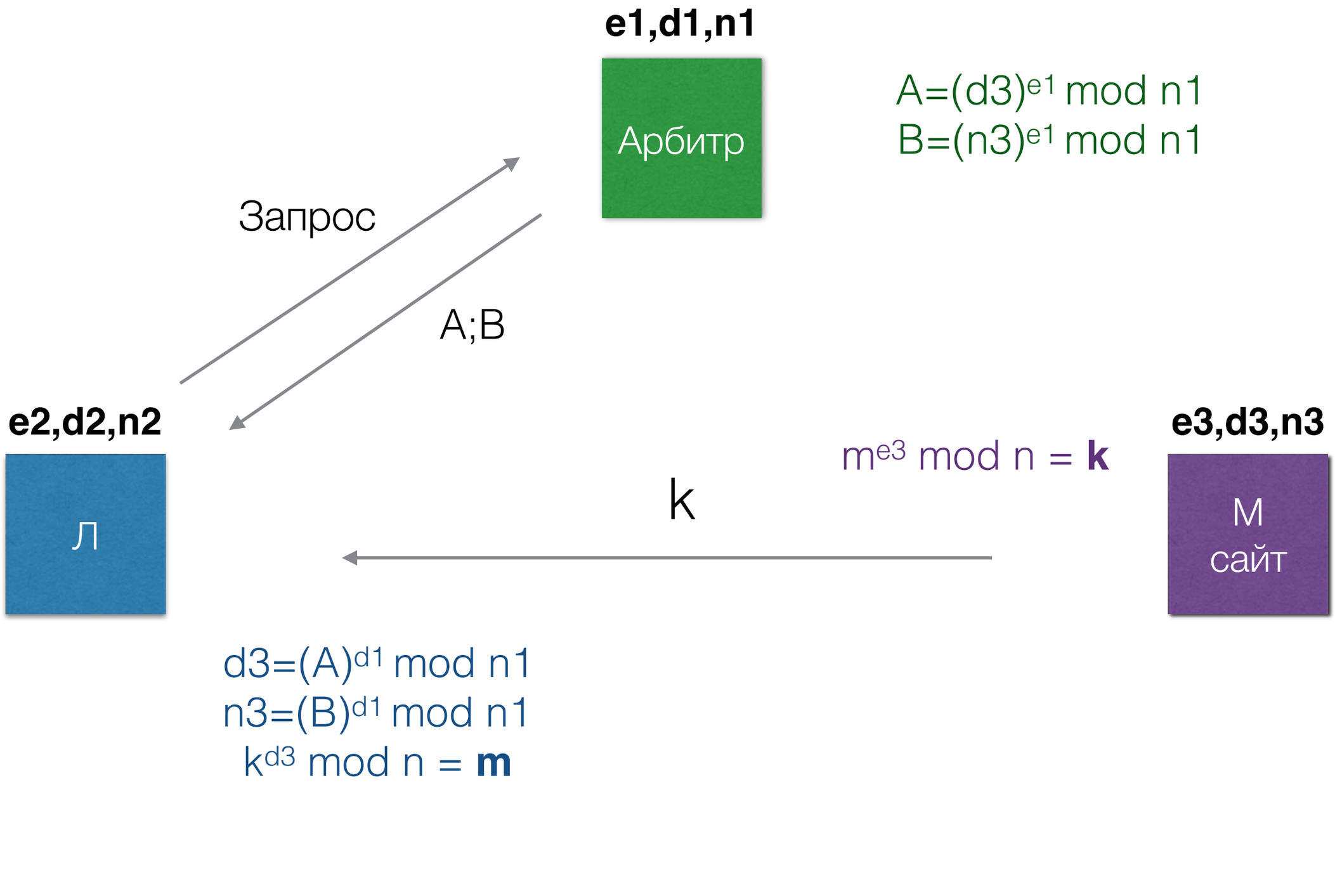
- «-У меня есть код, но я вам его не скажу» …
  «… -А как доказывать будете?»

- Позволяет реализовывать схемы с анонимными цифровыми платежами и голосованиями

Слепая ЭЦП


(m)e1 mod n = p
p
(p)e2 mod n = z
Л
z
М
(z)d1 mod n =
=((p)e2 mod n)d1 mod n =
=(((m)e1 mod n)e2 mod n)d1 mod n =
=(m)e2 mod n= ЭЦПл(m)

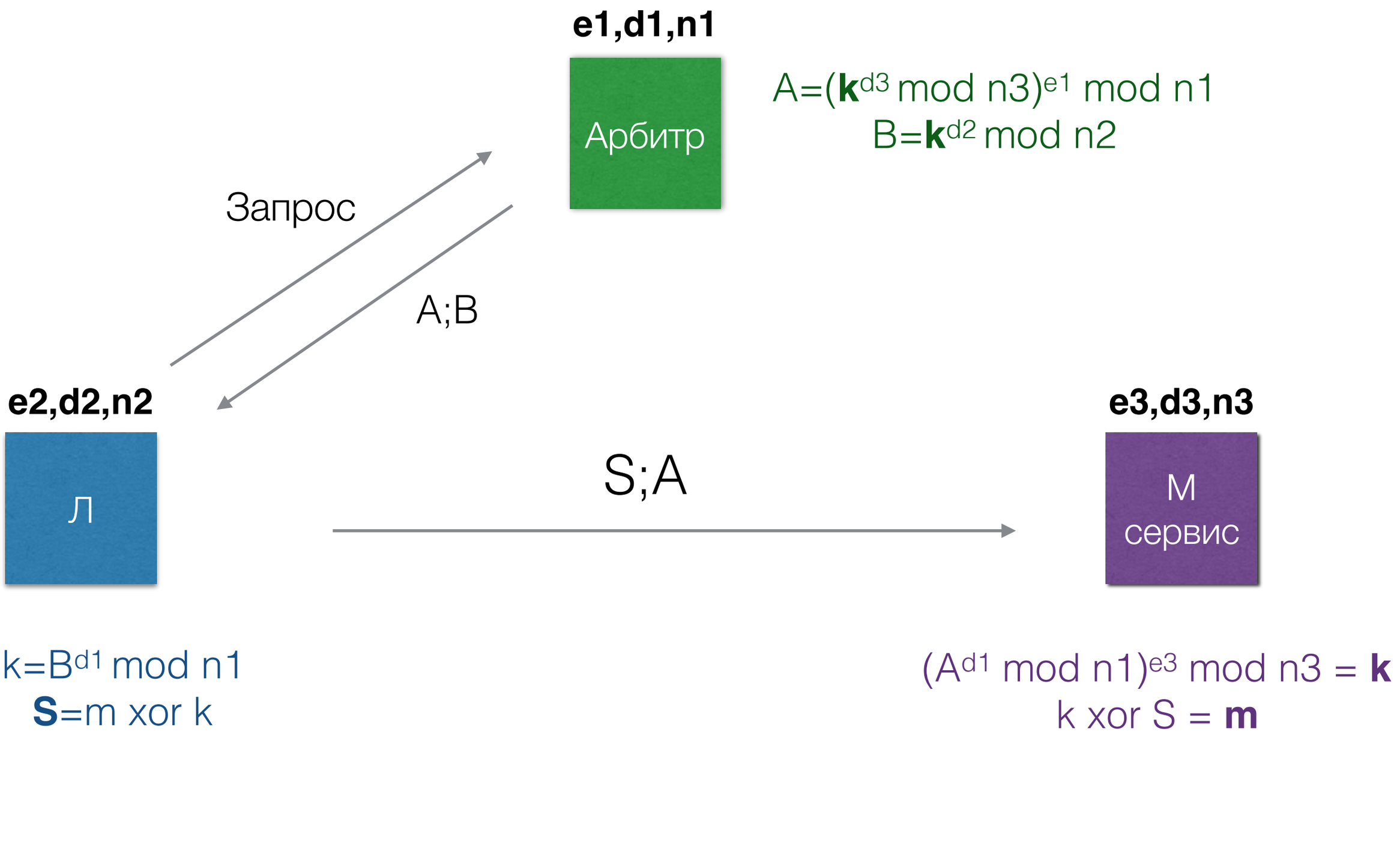
Сертификат


e1,d1,n1
Арбитр
A=(d3)^e1 mod n1
B=(n3)^e1 mod n1
Запрос
A;B
e2,d2,n2
Л
e3,d3,n3
m^e3 mod n = k
k
M
сайт
d3=(A)^d1 mod n1
n3=(B)^d1 mod n1
k^d3 mod n = m

Сертификат

- Подтверждает подлинность ключей
- Подтверждает подлинность собеседника/сайта
- Требует наличия доверенного арбитра

Мандат


e1,d1,n1
Арбитр
A=(k^d3 mod n3)^e1 mod n1
B=k^d2 mod n2
Запрос
A;B
e2,d2,n2
Л
S;A
e3,d3,n3
M
сервис
k=B^d1 mod n1
S=m xor k
(A^d1 mod n1)^e3 mod n3 = k
k xor S = m

Мандат

- Позволяет в одну операцию подтвердить:
  - подлинность отправителя
  - подлинность получателя
  - право/очередь отправителя на общение с получателем

Рецепты!

1. RSA открывается секретным ключом получателя
2. RSA закрывается публичным ключом получателя
3. ЭЦП открывается вскрывается публичным ключом отправителя
4. ЭЦП ставится секретным ключом отправителя
5. Сертификат содержит публичный ключ третьего лица. Вскрывается публичным ключом арбитра.
6. Самоподписанный сертификат тождественен ЭЦП
7. Мандат для отправителя: второе число вскрывается своим секретным ключом
8. Мандат для получателя: вскрывать сначала публичным ключом арбитра, затем секретным своим.