1 : 1 Messages

Alice

- A_0 (B_0)
- A_1
- Cipher 1 = [message (signed A_0), A_1] — Encrypted by B_0 →

Bob

- B_0 (A_0)
- verify w/ A_0 store A_1
- B_1 (A_1)

← Encrypted by A_1 — Cipher 2 = [message (signed B_0), B_1]

- verify w/ B_0 store B_1

- A_2 (B_1)

- Cipher 3 = [message (signed A_1), A_2] — Encrypted by B_1 →

- verify w/ A_1 store A_2

* What I'm trying to show from this diagram is that everytime a cipher text gets sent the recipent uses the old key to check the signature then stores the new one. They then create a new key and sign w/ the old key and attach the new one.

2 : 2 messages

Alice:

A_0 (B_0)

– A_1

– Cipher 1 = [message(signed A_0), A_1] → Encrypted w/ B_0

– A_2

– Cipher 2 = [message(signed A_1), A_2] → Encrypted w/ B_0

– Verify w/ B_0 store B_1 ← Encrypted w/ A_2

– (B_1)

– Verify w/ B_1 store B_2 ← Encrypted w/ A_2

– A_3 (B_2)

Bob:

– B_0 (A_0)

– Verify w/ A_0 store A_1

– (A_1)

– Verify w/ A_1 store A_2

– B_1 (A_2)

Cipher 3 = [Message(signed B_0), B_1]

– B_2

Cipher 4 = [Message(signed B_1), B_2]