Signcryption

- Goal: provides (confidentiality + authemtication)

- Encrypt-then-authenticate
- …Or, Authenticate-and-encrypt

- Inherits security properties of its parent schemes

Signcryption: Attempt 1

Encryption keys:(EK_A, DK_A)
Signing keys:(SK_A, VK_A)

Encryption keys:(EK_B, DK_B)
Signing keys:(SK_B, VK_B)

1. Do $C = EK_B(m)$
2. Send(Alice, C, $\sigma=Sign_{SKA}(C)$)

3. Strips off Alice's signature, replaces with (Charlie, C, $\sigma=Sign_{SKC}(C)$)
4. Bob won't notice anything amiss

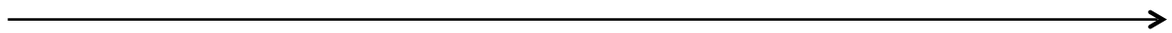
"Encrypt-then-authenticate" approach

Signcryption: Attempt 2

Encryption keys:(EK_A, DK_A)
Signing keys:(SK_A, VK_A)

Encryption keys:(EK_B, DK_B)
Signing keys:(SK_B, VK_B)

1. Do $\sigma = Sign_{SKA}(m)$
2. Compute $C = EK_B(m||\sigma)$
3. Send (Alice, C)



4. Do $(m||\sigma) \leftarrow DK_B(C)$
5. $Verify_{VKA}(m,\sigma) \stackrel{?}{=}$ "accept"

"Authenticate-then-encrypt" approach

Signcryption: Attempt 2

Encryption keys:(EK_A, DK_A)
Signing keys:(SK_A, VK_A)

Encryption keys:(EK_C, DK_C)
Signing keys:(SK_C, VK_C)

Encryption keys:(EK_B, DK_B)
Signing keys:(SK_B, VK_B)

1. Do $\sigma = Sign_{SKA}(m)$
2. Compute $C = EK_C(m||\sigma)$
3. Send(Alice,C) →
4. Do $(m||\sigma) \leftarrow DK_C(C)$
5. Compute (Alice, $C' = EK_B(m||\sigma)$)
6. Send(Alice,C′) →
7. Bob'll think (m,σ) came from Alice

"Authenticate-then-encrypt" approach

Signcryption

- Both attempt 1, 2 work
  - Attempt 1 fix: Step 1 — Alice does C = EK_B(Alice||m)
  - Attempt 2 fix: Step 1,2 — Alice does σ = $Sign_{SKA}$(Charlie||m), then compute C = EK_C(Alice||m||σ))
- Signing — include ID of recipient inside σ
- Encrypting — include ID of sender inside C
- Acronym: (E-S, S-R)

Rigorous treatment of signcryption: An, Dodis and Rabin, Eurocrypt'02