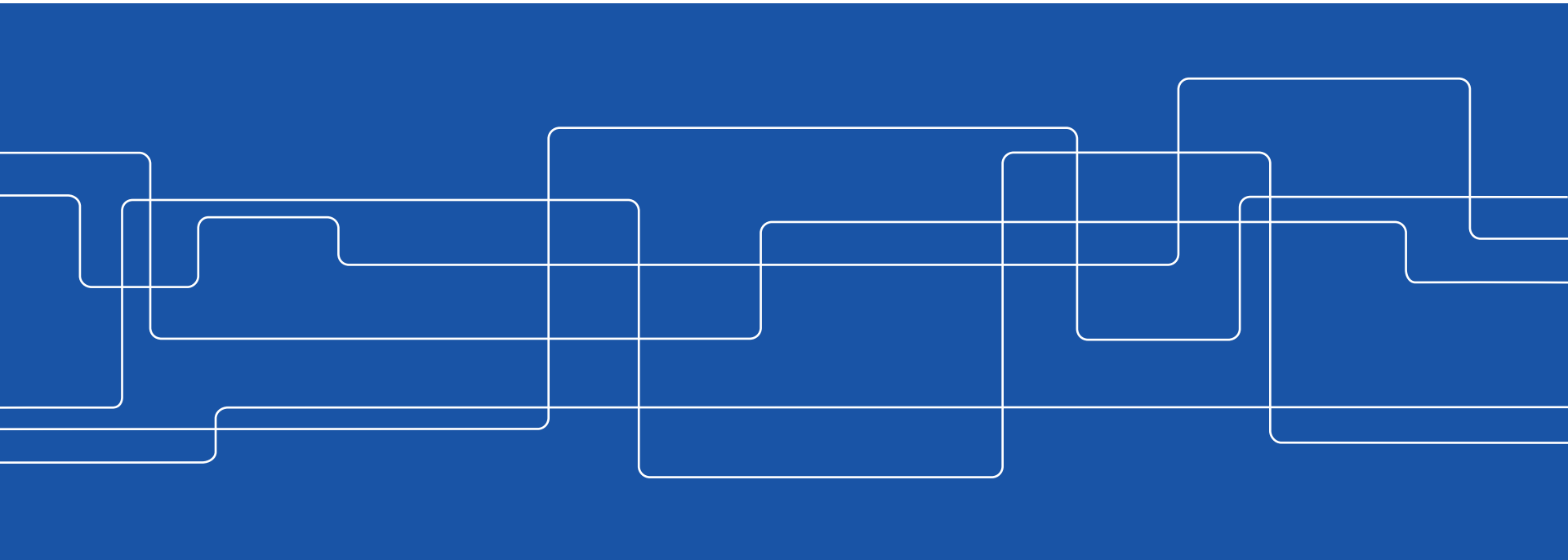
Digital Signatures

Göran Andersson

goeran@kth.se



Security Concepts

- ✓ Confidentiality
  - Encryption
- ✓ Integrity
  - Cryptographic checksums
- ➢ Authentication
  - Digital signatures

Signing with RSA

Alice wants to sign a message m and send it to Bob. Since Alice is the only one that knows d_A she can sign the message by encrypting with this key.

$$s \equiv_{n_A} m^{d_A}$$

By symmetry Bob can verify the message with Alice's public key (e_A, n_A).

$$m \equiv_{n_A} s^{e_A}$$

Explanation:

$$s^{e_A} = \left(m^{d_A}\right)^{e_A} = m^{e_A d_A} = m^{1+k\phi_A} = m\left(m^{\phi_A}\right)^k \equiv_{n_A} m\, 1^k = m$$

This is not a good idea if the message is a secret, since Bob and everyone else can read and verify that Alice wrote m.

Signing with RSA

Now, if Alice also wants to encrypt the message she can use Bob's public key. In order to avoid a risk of ambiguity we have to demand that $m < \min(n_A, n_B)$ and Alice should start with the key belonging to $\min(n_A, n_B)$. Now, assume that $n_A < n_B$.

$s \equiv_{n_A} m^{d_A}$ (sign)

$c \equiv_{n_B} s^{e_B}$ (encrypt)

Bob proceeds in reverse order, starting with the key belonging to $\max(n_A, n_B)$.

$s \equiv_{n_B} c^{d_B}$ (decrypt)

$m \equiv_{n_A} s^{e_A}$ (verify)

Problem

- Alice wants to send the code 112 to Bob. Of course she doesn't want anyone else to know this secret. She also wants Bob to be sure that she (and not Eve, if the keys where large) did send this code. What's the actual information sent over the communication channel?
- Show how Bob reveals the secret.

$$n_A = 667,\ e_A = 15$$

$$n_B = 589,\ e_B = 13$$

Signing with Elgamal

Recall that both Alice and Bob have published their (p, g, y) but keep x secret.

Now, Alice wants to sign m to Bob. She finds a session random number k which is invertible mod $\phi_A = p_A - 1$. The message m is signed with her public keys (p_A, g_A) and her private key x_A, by computing

$$c \equiv_{p_A} g_A^k$$

$$d \equiv_{\phi_A} k^{-1}(m - x_A\, c)$$

The signed message is the pair (c, d).

Bob verifies the message using the following test:

$$y_A^c\, c^d \equiv_{p_A} g_A^m \ ?$$

Instead of verifying the full message a digest $h(m)$ can be used instead of m.

Signing with Elgamal

Explanation, using Euler's theorem:

$$y_A^c\, c^d = \left(g_A^{x_A}\right)^c \left(g_A^k\right)^d = g_A^{c\,x_A + k\,d} = g_A^{c\,x_A + k\left(k^{-1}(m - x\,c) + n_1\,\phi_A\right)}$$

$$= g_A^{c\,x_A + k\,k^{-1}(m - x_A\,c) + k\,n_1\,\phi_A} = g_A^{c\,x_A + k\,k^{-1}(m - x_A\,c)} \left(g_A^{\phi_A}\right)^{k\,n_1}$$

$$\equiv_{p_A} g_A^{c\,x_A + (1 + n_2\,\phi_A)\,(m - x_A\,c)} \times 1 \equiv_{p_A} g_A^{m + n_2\,\phi_A\,(m - c\,x_A)}$$

$$= g_A^m \left(g_A^{\phi_A}\right)^{n_2\,(m - c\,x_A)} \equiv_{p_A} g_A^m \times 1 = g_A^m$$

Problem

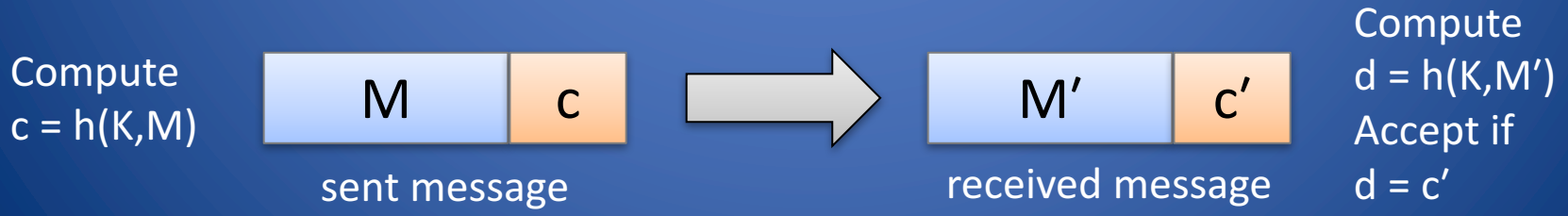
- Bob publish $(p, g, y) = (13, 6, 2)$ and keeps $x = 5$ secret.
  Alice generates $k = 5$ and wants to send $m = 5$.
  Help her!
- Alice has published $(p, g, y) = (31, 12, 15)$ and keeps $x = 9$ secret.
  Now she wants to sign m. Help her!

Signing with Hash Functions

- Signing full messages is inefficient
- In practical situation signing $H(m)$ is used instead
- Send the encrypted message
- And then the signed digest

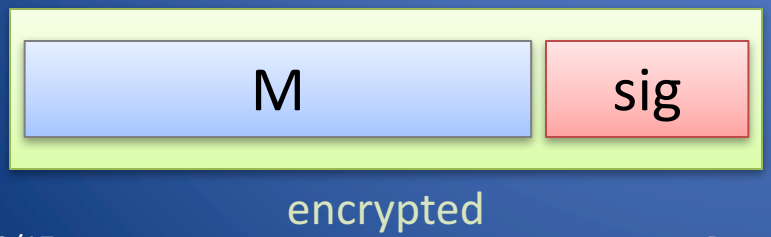
Message Authentication Code (MAC)

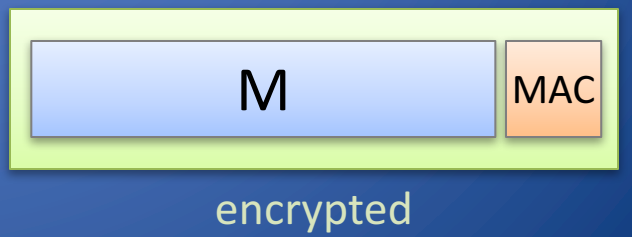
- Cryptographic hash function h(K,M) with two inputs:
  - Secret key K
  - Message M
- Message integrity with MAC
  - Sequence of messages transmitted over insecure channel
  - Secret key K shared by sender and recipient
  - Sender computes MAC c = h(K,M) and transmits it along with message M
  - Receiver recomputes MAC from received message and compares it with received MAC
  - Attacker cannot compute correct MAC for a forged message
  - More efficient than signing each message
  - Secret key can be sent in a separate encrypted and signed message



Securing a Communication Channel

- Assuring both integrity and confidentiality of messages transmitted over an insecure channel
- Sign and encrypt
  - The encrypted pair (message, signature) is transmitted
- MAC and encrypt
  - The encrypted pair (message, MAC) is transmitted
  - Secret key for MAC can be sent in separate message
  - More efficient than sign and encrypt
  - MAC is shorter and faster to compute than signature and verification
- Alternatively, signing or applying MAC could be done on encrypted message





Problem Session