Public Key Cryptography

RSA digital signatures &
the security of RSA

Public key authentication

• You can use public key to authenticate messages, as well as to encrypt them.
  – In the case of the RSA algorithm, if the sender “decrypts a message” instead of encrypting, it has the effect of a signature, as we shall see.
• Other public key algorithms have different mechanisms for encryption and authentication.

RSA signatures

• Bob’s RSA modulus is n, with public exponent e, and corresponding private exponent d. Remember:
  – n = pq, with p, q (private) primes; and
  – ed = 1 mod (p-1)(q-1).
• To authenticate message m, Bob computes:
  – s = m^d mod n
• Anybody may verify Bob’s signature s on m:
  – s^e mod n = m^{ed} mod n = m mod n.
Public key authentication

Bob’s private key

Public key authentication

Public key verification

Bob’s public key

(anybody’s) public key ring

Valid or Invalid

RSA and active attacks

• The algorithms we have described for public encryption and signatures using RSA are sometimes called “plain RSA.”
• Plain RSA is never used in practice, because of its inability to resist active attacks.

Malleability of plain RSA encryption

• Plain RSA encryption is malleable, because it can be changed.
• Suppose Alice sends ciphertext $c$ to Bob, but it is intercepted and changed to $c'$ by Eve.
• Bob decrypts:
  \[- m' \equiv c' d \mod n \]
• This is not the message sent by Alice. Unless $m'$ has special structure, Bob has no means of detecting the change.
Malleability

- Suppose Eve knows that Alice is reporting Eve’s salary to Bob’s payroll service firm.
  \[ c = (Eve\_salary)^e \mod n \]
- Mallory intercepts \( c \) and sends \( 2^e c \mod n \) instead. Bob decrypts:
  \[ (2^e c)^d = (2 \cdot Eve\_salary)^ed = 2 \cdot Eve\_salary \]

Redundancy

- In order to make RSA encryption secure against active attacks, redundancy must be provided.
- Example: if a 1024-bit RSA is used, one could force \( m \) to have 980 bits or fewer.
  \[ m = m^*2^{64} + p \mod n \]
  where \( p \) is a fixed 64-bit pattern.
- If ciphertext is tempered with a random modification, with probability \( 1 - 2^{-64} \) the modified ciphertext will NOT decrypt to a plaintext with the right bit pattern.
  \[ (a s)^e = c m \mod n \]
  This provides only heuristic security, as attacker will not necessarily use random alterations.

Malleability of RSA Signature

- Suppose Alice sends Bob a signed message:
  \[ (m, s), \text{where } s = m^d \mod n \]
- Eve intercepts the transmission and substitutes it with:
  \[ (c m, a s), \text{where } c = a^e \mod n \]
- Bob verifies that
  \[ (a s)^e = c m \mod n \]
  and accepts it as signed message from Alice.
- Redundancy is also need to for the security of RSA signatures against active attacks.