CRYPTOGRAPHY HANDOUT 18

DIGITAL SIGNATURES

1. First Explorations

Recall: cryptography is important because:

- Confidentiality: Only Bob should be able to read Alice's message.
- Data integrity: Alice's message shouldn't be altered in any way.
- Authentication: Bob wants to make sure Alice actually sent the message.
- Non-repudiation: Alice cannot claim she didn't send the message.

We have mostly spent time on confidentiality so far, but today we'll talk about the other three. Start by discussing with your group some specific scenarios in which these may arise.

Example. One example that might have come up is credit cards (e.g. signing a receipt and comparing to a credit card signature, chip and signature cards, chip and PIN cards).

Example. Digital signatures are for electronic documents (e.g. digital leases, tax documents, student loan documents).

Digital signature schemes consist of two steps:

1. Signing process
2. Verification process

We'll work through some digital signature schemes today.

Bob has a document m that Alice agrees to sign. Assume that m is not secret today.

2. RSA Signatures

1. Signing process
   a. Alice generates two large primes p and q. She computes $n = pq$.
   b. She chooses e_A such that $1 < e_A < \varphi(n)$ with $\gcd(e_A, \varphi(n)) = 1$.
   c. She computes d_A such that $e_A d_A \equiv 1 \bmod \varphi(n)$.
   d. Alice publishes (e_A, n) and keeps d_A, p, q private.
   e. Her signature is $y \equiv m^{d_A} \bmod n$. (m, y) are made public.
2. Verification process
   a. Bob gets Alice's (e_A, n). He computes $z \equiv y^{e_A} \bmod n$.
   b. If $z = m$, then Bob accepts the signature as valid. Otherwise, the signature is not valid.

Question 1. *Work through the RSA signature example with the following:*

- $p = 7, q = 13$
- $m = 35$

Suppose Eve wants to attach Alice's signature to another message m_1. She can't just use (m_1, y) since $y^{e_A} \not\equiv m_1 \bmod n$.

Question 2. *Show this using the example above. If $m_1 = 30$, what is $y^{e_A} \bmod n$?*

Since this doesn't match, then Alice didn't actually sign the document.

3. Blind Signatures - RSA

In some cases, a message is "blinded" or disguised before it is signed.

Example. Electronic voting systems might require that each ballot is certified by an election authority (Alice) before it can be accepted for counting. This allows Alice to check to make sure the voter (Bob) doesn't vote twice while also not being able to see the voter's actual ballot.

1. Alice chooses two primes p and q. Then she computes $n = pq$.
2. Alice also chooses an encryption exponent e and decryption exponent d.
3. (n, e) are public whereas p, q, d are private.
4. Bob chooses a random integer k mod n with $\gcd(k, n) = 1$ and computes $t \equiv k^e m \bmod n$. He sends t to Alice.
5. Alice signs t by computing $s \equiv t^d \bmod n$. She gives s to Bob.
6. Bob computes s/k mod n. This is the signed message m^d.

Question 3. *Show that s/k is actually the signed message m^d (i.e. show that $s/k \equiv m^d \bmod n$).*

4. ElGamal Signature Scheme

The ElGamal Encryption method can also be modified to give a signature scheme.

Before she gets started, Alice chooses a prime p and a primitive root α. She chooses a secret integer a such that $1 \leq a \leq p-2$ and calculates $\beta \equiv \alpha^a \bmod p$. (p, α, β) are made public while a is private.

1. Signing process
   - a. Alice chooses a secret random k such that $\gcd(k, p-1) = 1$.
   - b. She computes $r \equiv \alpha^k \bmod p$ with $0 < r < p$.
   - c. She also computes $s \equiv k^{-1}(m - ar) \bmod (p-1)$. The signed message is (m, r, s).
2. Verification process
   - a. Bob gets Alice's public key (p, α, β).
   - b. He computes $v_1 \equiv \beta^r r^s \bmod p$ and $v_2 \equiv \alpha^m \bmod p$.
   - c. The signature is valid if and only if $v_1 \equiv v_2 \bmod p$.

Question 4. *Show that the verification process works. Assume the signature is valid with the following steps:*

- *Since* $s \equiv k^{-1}(m - ar) \bmod p-1$, *then* $sk \equiv$ ____________ $\bmod (p-1)$.

- *This means* $m \equiv$ __________________ $\bmod (p-1)$.

- *A congruence* $\bmod p-1$ *in the exponent yields an overall congruence* $\bmod p$, *so we have:*

  $v_2 \equiv \alpha^m \equiv$ ____________________________________ $\equiv v_1 \bmod p$