CRYPTOGRAPHY HANDOUT 18

DIGITAL SIGNATURES (GUIDED NOTES)

1. RSA Signatures

Bob has a document or message m that Alice agrees to sign.

1. Signing process
   a. Alice generates two large primes p and q. She computes $n = pq$.
   b. She chooses e_A where $1 < e_A < \varphi(n)$ 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.

Example. $m = 35$

1. Signing process: $p = 7, q = 13$
   a. $n =$ ____________
   b. $\varphi(n) =$ ____________ $e_A =$ ____________
   c. $d_A =$ ____________
   d. Public info: $(e_A, n) =$ ____________
   e. Alice's Signature: $y =$ ____________
2. Verification Process: Bob sees (e_A, n) and $(m, y) =$ ____________.
   (a) He computes $z =$ ____________
   (b) Is the signature valid or not?

Example. $m = 14$

1. Signing process: $p = 11, q = 17$
   a. $n =$ ____________
   b. $\varphi(n) =$ ____________ $e_A = 7$ works here because $\gcd(7, \varphi(n)) =$ ____________
   c. $d_A = 183$ works here because $e_A d_A \equiv 1 \bmod \varphi(n)$. Check this: ____________
   d. Public info: $(e_A, n) =$ ____________
   e. Alice's Signature: $y =$ ____________
2. Verification Process: Bob sees (e_A, n) and $(m, y) =$ ____________.
   (a) He computes $z =$ ____________
   (b) Is the signature valid or not?

What if during the verification process, Bob had received $(m, y) = (14, 158)$ instead? What would he conclude?

2. Blind Signatures - RSA

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

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, which is m^d.

Example. $m = 11$

1. $p = 7, q = 13$, so $n = pq =$ ____________
2. $e = 5$ and $d = 29$ because $de \equiv 1 \bmod \varphi(n)$. Verify this: ____________
3. $(n, e) =$ ____________
4. $k =$ ____________ since $\gcd(k, n) = 1$. He computes $t =$ ____________
5. $s =$ ____________
6. $s/k =$ ____________ which should match up with $m^d =$ ____________

Example. $m = 23$

1. $p = 11, q = 17$, so $n = pq =$ ____________
2. $e = 7$ and $d = 183$ because $de \equiv 1 \bmod \varphi(n)$. Verify this: ____________
3. $(n, e) =$ ____________
4. $k =$ ____________ since $\gcd(k, n) = 1$. He computes $t =$ ____________
5. $s =$ ____________
6. $s/k =$ ____________ which should match up with $m^d =$ ____________

Question 1. *Show that s/k is actually the signed message m^d.*

3. 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 $v_1 \equiv v_2 \bmod p$.

Example. Before she gets started, Alice chooses a prime $p = 17$ and a primitive root $\alpha = 3$. She chooses a secret integer $a = 4$ such that $1 \leq a \leq p - 2$ and calculates $\beta \equiv \alpha^a \bmod p =$ ____________. $(p, \alpha, \beta) =$ ____________ are made public while a is private.

1. Signing process
   a. $k = 5$ since $\gcd(k, p - 1) = 1$. Verify this: ____________.
   b. $r =$ ____________
   c. $s =$ ____________. The signed message is $(m, r, s) =$ ____________.
2. Verification process
   a. Bob gets Alice's public key (p, α, β).
   b. $v_1 =$ ____________ and $v_2 =$ ____________.
   c. The signature is valid if and only if $v_1 \equiv v_2 \bmod p$.

Question 2. *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:*