

CIS 4362/MAT 5932
Introduction to Cryptology and Information Security

Homework #3

November 3, 2008

Please hand in your solution no later than November 14, 2008, 2:07 p.m.
Solutions handed in after this deadline will be graded with 0 points.

Problem 1 Identity-based signing (CIS 4362 and MAT 5932) 10 Points

As discussed in class, in an identity based signature scheme, there is a (user-independent) set of public system parameters, and users have no individual public verification keys. To verify signatures from a user, knowing its identity—e.g., Alice.Smith@fau.edu—is sufficient. To extract private user keys from arbitrary user identities, a key generation center is available. Users have to contact this center to obtain their private signing key.

(a) (CIS 4362 and MAT 5932)

Building on the signature scheme RSA-FDH (a message m is signed as $H(m)^d \bmod n$), explain how an identity-based signature scheme can be realized.

(b) (CIS 4362 and MAT 5932)

Using small toy parameters ($2^{20} < n < 2^{160}$), compute a signature on your first name that can be verified with the user identity that is equal to your last name. (To represent letters as bitstrings you can identify letters with numbers in the range $\{0, \dots, 25\}$, then use a binary representation of fixed length 5, i.e., A – “00000”, B – “00001”, ..., Z – “11001”.)

Hint: In Magma, an implementation of the hash function SHA-1 is available. For instance, to hash the bitstring “011” the command `SHA1 (“011”)` can be used.

(c) (MAT 5932 only)

If the secret signing key of a user is compromised, a possibility to revoke such a key is needed. Suppose we derive user identities from email addresses. How could the problem of key revocation be addressed without forcing users to change their email address when their secret signing key has been revealed?

Problem 2 Identity-based encryption (CIS 4362 and MAT 5932)**5 Points**

In class we discussed an identity-based encryption scheme of Boneh and Franklin. In the notation from class, the ciphertext has the form

$$c = (r \cdot P, \sigma \oplus H_2(g_{id}^r), m \oplus H_4(\sigma))$$

with uniformly at random chosen $r \in \{1, \dots, q-1\}$, $\sigma \in \{0, 1\}^n$, and where $g_{id} = e(Q_{id}, sk \cdot P)$, Q_{id} is a curve point depending on the user identity id , $sk \cdot P$ is part of the public system parameters, the H_i s are public hash functions, and m is the plaintext. Explain how the secret key $sk \cdot Q_{id}$ can be used to recover the plaintext message m from the ciphertext.

Problem 3 Elliptic curves (CIS 4362 and MAT 5932)**5 Points**

One of the most popular signing algorithms is ECDSA, the elliptic curve version of the digital signature algorithm. Suppose you want to make sure that your signature cannot be forged in the next ten year—this is desirable for electronic signatures on passports, for instance. Suggest realistic parameters (“which curve?”) for the ECDSA algorithm that could be suitable for such an application.

Good luck—and have fun!!