

CS355: Cryptography

Lecture 22: Mental
Poker. Pohlig-Hellman.
Quadratic residues.

Midterm

7:00–9:00 PM

Wed. Feb 28, 2007

ME 261

The Mental Poker Problem

- Alice and Bob want to play poker, deal 5 cards to each of Alice and Bob so that
 - Alice's hand of 5 cards does not overlap with Bob's hand
 - Neither Alice nor Bob can control which cards they each get
 - Neither Alice nor Bob knows the other party's hand
 - Both hands should be random provided one party follows the protocol
- First solution due to Shamir, Rivest, and Adelman in 1980 (SRA protocol)
 - uses commutative encryption schemes

Commutative Encryption

Definition:

An encryption scheme is commutative if

$$E_{K_1}[E_{K_2}[M]] = E_{K_2}[E_{K_1}[M]]$$

Given an encryption scheme that is commutative, then

$$D_{K_1}[D_{K_2}[E_{K_1}[E_{K_2}[M]]] = M$$

**Most symmetric encryption scheme
(such as DES and AES) are not commutative**

Pohlig-Hellman Exponentiation Cipher

- A commutative encryption scheme
- Pohlig-Hellman Exponentiation Cipher with the same modulus p , p prime
 - encryption key is e , decryption key is d , where $ed \equiv 1 \pmod{p-1}$
 - $E_{e_1}[M] = M^{e_1} \pmod{p}$ and $D_{d_1}[C] = C^{d_1} \pmod{p}$
 - $E_{e_1}[E_{e_2}[M]] = M^{e_1 e_2} = E_{e_1}[E_{e_2}[M]] \pmod{p}$

The SRA encryption scheme

- Commutative encryption
- Alice and Bob share $n=pq$ and they both know p and q
- Alice: encryption key e_1
decryption key d_1
 $e_1 d_1 \equiv 1 \pmod{(p-1)(q-1)}$
- Bob: encryption key e_2
decryption key d_2
 $e_2 d_2 \equiv 1 \pmod{(p-1)(q-1)}$

The SRA Mental Poker Protocol

Setup: Alice and Bob share M_1, M_2, \dots, M_{52} denote the 52 cards, $n=pq$, p , and q .
Alice has e_1, d_1 and Bob has e_2, d_2

Protocol:

- Alice encrypts M_1, M_2, \dots, M_{52} using her key, i.e., computes $C_j = M_j^{e_1} \pmod n$ for $1 \leq j \leq 52$, randomly permute them and send the ciphertexts to Bob
- Bob picks 5 cards as Alice's hand and sends them to Alice
- Alice decrypts them to get her hand
- Bob picks 5 other cards as his hand, encrypts them using his key, and sends them to Alice
- Alice decrypts the 5 ciphertexts and sends to Bob
- Bob decrypts what Alice sends and gets his hand
- Both Alice and Bob reveal their key pairs to the other party and verify that the other party was not cheating.

“Security Analysis” of the Protocol

- Bob sees 52 random ciphertexts, he doesn't know which ciphertext corresponds to which card.
- Bob can only randomly pick Alice's hand, and Bob does not know what Alice's hand is.
- Bob can only randomly pick his hand, and Alice doesn't know Bob's hand, as it is encrypted under Bob's key.
- **This is not a security proof.**

Quadratic Residues

a is a quadratic residue modulo p if $\exists b \in \mathbb{Z}_p^*$ such that $b^2 \equiv a \pmod{p}$, otherwise a is a nonquadratic residue

Q_p is the set of all quadratic residues

\overline{Q}_p is the set of all nonquadratic residues

- If p is prime there are $(p-1)/2$ quadratic residues in \mathbb{Z}_p^* , $|Q_p| = (p-1)/2$
- If $a^{(p-1)/2} \equiv 1 \pmod{p}$ then a is a quadratic residue (if -1 then r is a nonquadratic residue)

Legendre Symbol

- Let p be an odd prime and a an integer. The Legendre symbol is defined

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a \\ 1, & \text{if } a \in Q_p \\ -1, & \text{if } a \in \overline{Q}_p \end{cases}$$

Jacobi Symbol

- let $n \geq 3$ be a **composite** odd with prime factorization

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

- the Jacobi symbol is defined to be

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k}$$

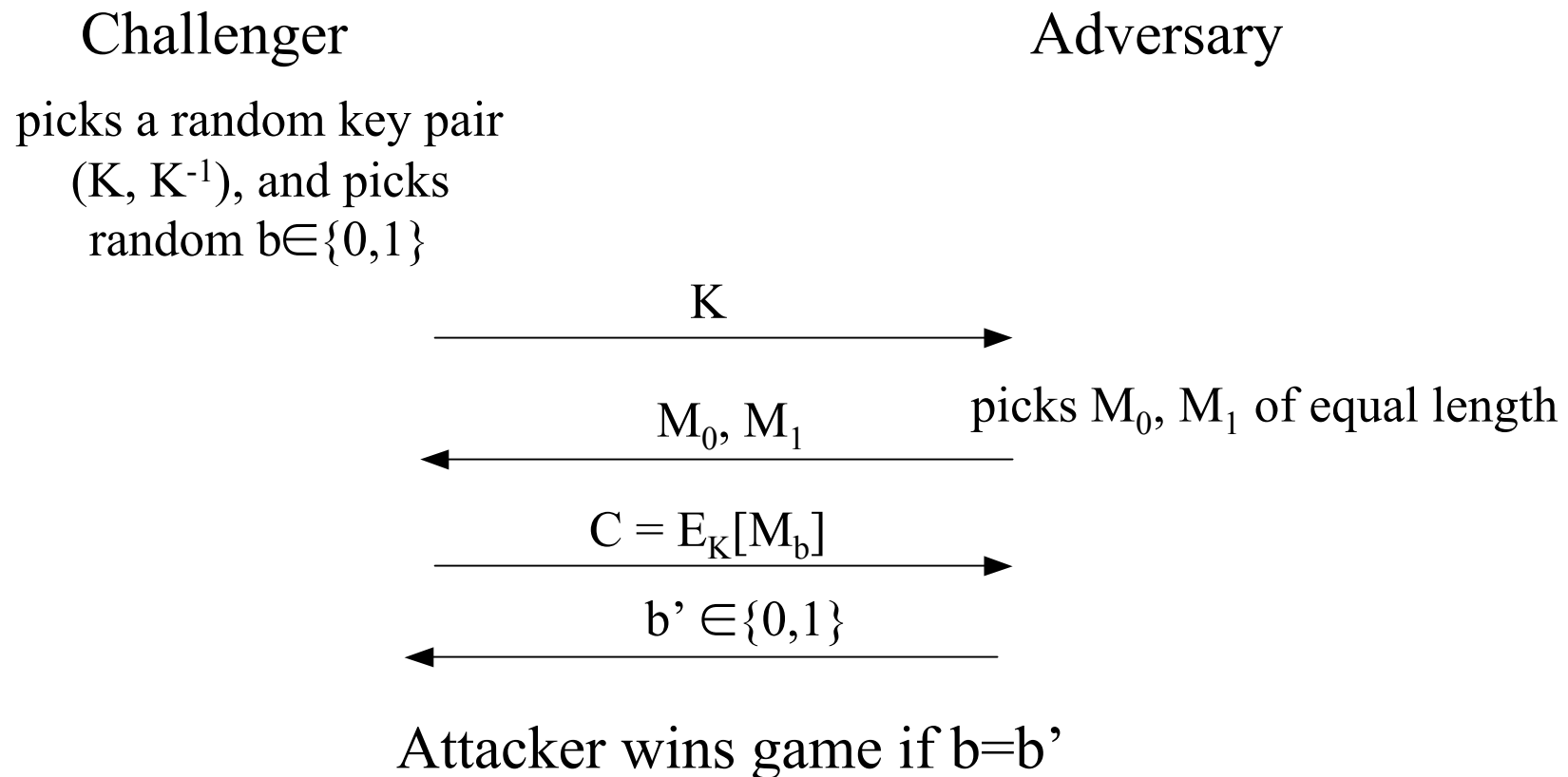
The Jacobi symbol can be computed without factoring n

AN ATTACK ON THE SRA MENTAL POKER Protocol

- The encryption function $f(x)=x^e \pmod n$ leaks information about x !
 - $f(x)$ is QR modulo n iff. x is QR modulo n
 - $x^e \in \text{QR}_n \Leftrightarrow x^e \in \text{QR}_p$ and $x^e \in \text{QR}_q \Leftrightarrow x \in \text{QR}_p$ and $x \in \text{QR}_q \Leftrightarrow x \in \text{QR}_n$
 - Why this matters in the SRA mental poker protocol?
 - suppose that the cards that are QR are mostly large cards, and the cards that are not QR are mostly small cards, then Bob can choose large cards for him and small cards for Alice

Semantic Security (IND-CPA for Public Key Encryption)

- The IND-CPA game



Semantic Insecurity of the RSA

- RSA encryption is not semantically secure because it is deterministic
- The encryption function $f(x)=x^e \bmod n$ leaks information about x !
 - it leaks the Jacobi symbol of x , so it allows an attacker to distinguish between ciphertexts

$$\left(\frac{x^e}{N}\right) = \left(\frac{x^e}{p}\right)\left(\frac{x^e}{q}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{q}\right) = \left(\frac{x}{N}\right)$$