Games

Cryptography – CS 507
Erkay Savas
Sabanci University
erkays@sabanciuniv.edu
Flipping Coins over the Telephone

- Alice and Bob wants to flip a coin to decide who will get the car that their friends left them in his will.
- Bob is in charge of flipping coins.
- Alice chooses *Tails* and Bob flips the coin.
- Independent of the outcome, Bob always tells Alice “Sorry, it was Heads.”
- Alice has all the rights to suspect that Bob is lying.
- Cryptography saves them by providing a fair protocol.
Flipping coins … : The Protocol

1. Alice chooses two large primes \( p \) and \( q \) s.t. \( p, q \equiv 3 \pmod{4} \). She keeps \( p \) and \( q \) secret, but sends \( n = pq \) to Bob.

2. Bob chooses a random integer \( x \pmod{n} \) and computes
   \[ y \equiv x^2 \pmod{n}. \]
   He keeps \( x \) secret and sends \( y \) to Alice.

3. Alice calculates the four square roots \( \pm a \) and \( \pm b \) of \( y \pmod{n} \). She does not know which one is \( x \).

4. She chooses one at random, say \( b \), and sends it to Bob.
Flipping coins … : The Protocol

5. If \( b \equiv \pm x \pmod{n} \), Bob tells Alice that she wins. If \( a \equiv \pm x \pmod{n} \), Bob wins.

6. When Bob wins, he can prove this by factoring \( n \).
   - If Alice sends \( b \) to Bob and \( x \equiv \pm a \pmod{n} \), then Bob knows all four square roots of \( y \), hence he can factor \( n \).
   - Can Alice cheat?
   - She can send Bob a number which is not a square root of \( y \).
     - Bob can easily detect it.
Can Alice cheat?

• Alice tries to cheat Bob by sending a product of three primes.
• Bob could ask the factorization of the modulus at the end of the protocol. Alice produces two factors that can be easily checked for primality.
• However, on the other hand, Bob shouldn’t be worried about this possibility. When \( n \) is a product of three primes, there are eight square roots of \( y \). Each of the three wrong choices will allow Bob to find a nontrivial factor of \( n \).
• Alice also decreases her chance of winning from \( \frac{1}{2} \) to \( \frac{1}{4} \).
Flipping coins over telephone

- If Bob decides to lose, he tells Alice she wins even though he can factor $n$.

- **Example**: Alice chooses
  
  $p = 2038074743$ and $q = 1190494759$
  
  and she sends
  
  $n = pq = 2426317299991771937$
  
  to Bob.

- Bob selects at random
  
  $x = 1414213562373095048$
  
  and computes
  
  $y \equiv x^2 \equiv 363278601055491705 \pmod{n}$.
  
  which he sends to Alice.
Example

• Alice computes
  \[y^{(p+1)/4} \equiv 1701899961 \pmod{p}\] and
  \[y^{(q+1)/4} \equiv 325656728 \pmod{q}\].

• Using CRT, she computes four square roots of \(y \pmod{n}\).
  \[x \equiv \pm 1012103737618676889 \pmod{n}\] or
  \[x \equiv \pm 937850352623334103 \pmod{n}\]

• Suppose Alice sends 1012103737618676889 to Bob.
• Since this is \(-x \pmod{n}\), Bob has to declare that Alice is the winner.
Example

• If she sent $937850352623334103$ to Bob, he would compute a nontrivial factor of $n$ by
  \[ \text{gcd}(1414213562373095048 - 937850352623334103, n) = 1190494759 = q. \]

• So he can prove he won.
Poker over the Telephone

• Alice and Bob can even play poker over the phone.

1. Alice and Bob agree on a large prime $p$.

2. Alice chooses a secret integer $\alpha$ with $\text{gcd}(\alpha, p-1) = 1$ 
   & she computes $\alpha'$ s.t. $\alpha\alpha' \equiv 1 \pmod{p-1}$

3. Bob chooses a secret integer $\beta$ with $\text{gcd}(\beta, p-1) = 1$ 
   & he computes $\beta'$ s.t. $\beta\beta' \equiv 1 \pmod{p-1}$.
   (Note that $c^{\alpha'\alpha} \equiv c \pmod{p}$) and (Note that $c^{\beta'\beta} \equiv c \pmod{p}$)

4. 52 cards are mapped into 52 distinct numbers
   $c_1, c_2, \ldots, c_{52} \pmod{p}$. 
5. Bob computes $b_i \equiv c_i^\beta \pmod{p}$ for $1 \leq i \leq 52$, randomly permutes these numbers and sends them to Alice.

6. Alice chooses five numbers $b_{i_1}, b_{i_2}, b_{i_3}, b_{i_4}, b_{i_5}$ and computes $b_{i_j}^\alpha \pmod{p}$ for $1 \leq j \leq 5$. and send these numbers to Bob.

7. Bob takes off his lock by raising these numbers to the power of $\beta'$. 

$$
\left( \left( b_{i_j}^\alpha \right)^{\beta'} \right)^\alpha \equiv \left( c_{i_j}^{\beta'} \right)^\alpha \equiv c_{i_j}^\alpha \pmod{p} \quad \text{for } 1 \leq j \leq 5.
$$
Poker over the Telephone

7. Bob sends \( c_{i,j}^\alpha \pmod{p} \) for \( 1 \leq j \leq 5 \) back to Alice.

8. Alice removes her lock by raising these numbers to the power of \( \alpha' \). This gives Alice her hand, which is \( c_{i_1}, c_{i_2}, c_{i_3}, c_{i_4}, c_{i_5} \).

9. Alice then chooses five more of the numbers \( b_i \) and sends them to Bob, who removes his lock. Resulting numbers constitute Bob’s hand.
Security of the protocol.

- For Alice, it seems to be difficult to deduce Bob’s cards since to do that she needs to calculate the discrete logarithm a large modulo.
- i.e. she needs to solve

\[ b_{ij} \equiv c_{ij}^\beta \pmod{p} \text{ for any } j \in [1, 5]. \]
Poker over the phone: Example

- A simplified poker with five cards: Ten, Jack, Queen, King, and Ace.
- Each player is dealt one card.
- The winner is the one with higher card.
- Mapping cards to integers:
  - Ten → 200514
  - Jack → 10010311
  - Queen → 1721050514
  - King → 11091407
  - Ace → 10305
Poker over the phone: Example

- Let the prime \( p = 2396271991 \).
- Alice chooses \( \alpha = 1234567 \) (secret) => \( \alpha' = 402406273 \)
- Bob chooses \( \beta = 7654321 \) (secret) => \( \beta' = 200508901 \).
- Bob now calculates
  
  Ten     : \( 200514\beta \pmod{p} \equiv 914012224 \)
  Jack    : \( 10010311\beta \pmod{p} \equiv 1507298770 \)
  Queen   : \( 1721050514\beta \pmod{p} \equiv 74390103 \)
  King    : \( 11091407\beta \pmod{p} \equiv 2337996540 \)
  Ace      : \( 10305\beta \pmod{p} \equiv 1112225809 \)
Poker over the phone: Example

• Bob shuffles these numbers and send them to Alice: 1507298770, 1112225809, 2337996540, 914012224, 74390103.
• Alice chooses one of these numbers and raises it to the power of $\alpha = 1234567$ and sends the result to Bob: $914012224^\alpha \equiv 1230896099 \pmod{p}$.
• Alice also chooses one card for Bob’s hand, say 1507298770
• Bob takes his lock off and sends the result back to Alice
  $1230896099^\beta \equiv 1700536007 \pmod{p}$. 
Poker over the phone: Example

• Alice removes her lock
  \[1700536007^\alpha \equiv 200514 \pmod{p}\]
  \(\Rightarrow\) Her card is Ten.

• Bob removes his lock from his own hand
  \[1507298770^\beta \equiv 10010311 \pmod{p}\]
  \(\Rightarrow\) His card is Jack.

• Jack wins.
How to cheat in poker?

• A number $r$ is called a \textit{quadratic residue} mod $p$ if it is a square mod $p$. Otherwise it is called \textit{nonresidue}.

• It is easy to check a nonzero number if it is a quadratic residue or nonresidue mod $p$.

$$z^{(p-1)/2} \equiv \begin{cases} +1 \pmod{p} & \text{if } z \text{ is a quadratic residue} \\ -1 \pmod{p} & \text{if } z \text{ is a quadratic nonresidue} \end{cases}$$

• Recall that we needed $\gcd(\alpha, p-1) = \gcd(\beta, p-1) = 1$. Therefore, $\alpha$ and $\beta$ are odd numbers.
How to cheat in poker?

- A card $c$ is encrypted to $c^\beta$, and
  \[
  \left(c^\beta\right)^{(p-1)/2} \equiv \left(c^{(p-1)/2}\right)^\beta \equiv c^{(p-1)/2} \pmod{p}
  \]
  since $(\pm 1)^{\text{odd}} = \pm 1$.
- Therefore, $c$ is a quadratic residue mod $p$ if and only if $c^\beta$ is a quadratic residue.
- It applies to $\alpha$ and $\alpha \beta$ powers of the cards.
- When Alice sends Bob the five cards that will make up her hand, Bob can check if these cards are quadratic residue ($\mathbf{R}$) or nonresidue ($\mathbf{N}$).
- This gives Bob a slight advantage.
How to cheat in poker?

• For example, suppose he needs to know whether or not she has the Queen of Hearts which he determines is in $N$.

• If none of her cards is in $N$, he will know she does not have the Queen of Hearts.

• If there are many cards in deck that are in $N$ and she has only one card in $N$, then the odds are quite low she has the Queen of Hearts.

• In a game such as poker, this slight advantages might give Bob many opportunities to win the game in the long run.
How to cheat in poker?

- Alice can cheat as well.
- She arranges all the cards that are in $R$, for example, when she chooses Bob’s hand.
- Then she knows that Bob’s hand is chosen from 26 cards rather than 52.
- Or she can arrange the prime $p$ so that the Ace, King, Queen, Jack, and Ten of Spades are the quadratic residues.
- When she chooses Bob’s hand she gives him five nonresidues.
- She picks herself all the residues to increase her chance of winning