

University of Rochester
CSC290B
Introduction to Computer Security

Asymmetric Cryptography

March 26, 2009

Public Key Cryptography

- Two keys
 - *Private key* known only to individual
 - *Public key* available to anyone
 - Public key, private key inverses
- Idea
 - Confidentiality: encipher using public key, decipher using private key
 - Integrity/authentication: encipher using private key, decipher using public one

Requirements

1. It must be computationally easy to encipher or decipher a message given the appropriate key
2. It must be computationally infeasible to derive the private key from the public key
3. It must be computationally infeasible to determine the private key from a chosen plaintext attack

Diffie-Hellman

- Compute a common, shared key
 - Called a *symmetric key exchange protocol*
- Based on discrete logarithm problem
 - Given integers n and g and prime number p , compute k such that $n = g^k \pmod{p}$
 - Solutions known for small p
 - Solutions computationally infeasible as p grows large

Algorithm

- Constants: prime p , integer $g \neq 0, 1, p-1$
 - Known to all participants
- Anne chooses private key k_{Anne} , computes public key $K_{Anne} = g^{k_{Anne}} \bmod p$
- To communicate with Bob, Anne computes $K_{shared} = K_{Bob}^{k_{Anne}} \bmod p$
- To communicate with Anne, Bob computes $K_{shared} = K_{Anne}^{k_{Bob}} \bmod p$
 - It can be shown these keys are equal

Example

- Assume $p = 53$ and $g = 17$
- Alice chooses $k_{Alice} = 5$
 - Then $K_{Alice} = 17^5 \bmod 53 = 40$
- Bob chooses $k_{Bob} = 7$
 - Then $K_{Bob} = 17^7 \bmod 53 = 6$
- Shared key:
 - $K_{Bob}^{k_{Alice}} \bmod p = 6^5 \bmod 53 = 38$
 - $K_{Alice}^{k_{Bob}} \bmod p = 40^7 \bmod 53 = 38$

RSA

- Exponentiation cipher
- Relies on the difficulty of determining the number of numbers relatively prime to a large integer n

Background

- Totient function $\phi(n)$
 - Number of positive integers less than n and relatively prime to n
 - *Relatively prime* means with no factors in common with n
- Example: $\phi(10) = 4$
 - 1, 3, 7, 9 are relatively prime to 10
- Example: $\phi(21) = 12$
 - 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20 are relatively prime to 21

Algorithm

- Choose two large prime numbers p, q
 - Let $n = pq$; then $\phi(n) = (p-1)(q-1)$
 - Choose $e < n$ such that e is relatively prime to $\phi(n)$.
 - Compute d such that $ed \bmod \phi(n) = 1$
- Public key: (e, n) ; private key: d
- Encipher: $c = m^e \bmod n$
- Decipher: $m = c^d \bmod n$

Example: Confidentiality

- Take $p = 7$, $q = 11$, so $n = 77$ and $\phi(n) = 60$
- Alice chooses $e = 17$, making $d = 53$
- Bob wants to send Alice secret message HELLO
(07 04 11 11 14)
 - $07^{17} \bmod 77 = 28$
 - $04^{17} \bmod 77 = 16$
 - $11^{17} \bmod 77 = 44$
 - $11^{17} \bmod 77 = 44$
 - $14^{17} \bmod 77 = 42$
- Bob sends 28 16 44 44 42

Example

- Alice receives 28 16 44 44 42
- Alice uses private key, $d = 53$, to decrypt message:
 - $28^{53} \bmod 77 = 07$
 - $16^{53} \bmod 77 = 04$
 - $44^{53} \bmod 77 = 11$
 - $44^{53} \bmod 77 = 11$
 - $42^{53} \bmod 77 = 14$
- Alice translates message to letters to read HELLO
 - No one else could read it, as only Alice knows her private key and that is needed for decryption

Example: Integrity/Authentication

- Take $p = 7$, $q = 11$, so $n = 77$ and $\phi(n) = 60$
- Alice chooses $e = 17$, making $d = 53$
- Alice wants to send Bob message HELLO (07 04 11 11 14) so Bob knows it is what Alice sent (no changes in transit, and authenticated)
 - $07^{53} \bmod 77 = 35$
 - $04^{53} \bmod 77 = 09$
 - $11^{53} \bmod 77 = 44$
 - $11^{53} \bmod 77 = 44$
 - $14^{53} \bmod 77 = 49$
- Alice sends 35 09 44 44 49

Example

- Bob receives 35 09 44 44 49
- Bob uses Alice's public key, $e = 17$, $n = 77$, to decrypt message:
 - $35^{17} \bmod 77 = 07$
 - $09^{17} \bmod 77 = 04$
 - $44^{17} \bmod 77 = 11$
 - $44^{17} \bmod 77 = 11$
 - $49^{17} \bmod 77 = 14$
- Bob translates message to letters to read HELLO
 - Alice sent it as only she knows her private key, so no one else could have enciphered it
 - If (enciphered) message's blocks (letters) altered in transit, would not decrypt properly

Example: Both

- Alice wants to send Bob message HELLO both enciphered and authenticated (integrity-checked)
 - Alice's keys: public (17, 77); private: 53
 - Bob's keys: public: (37, 77); private: 13
- Alice enciphers HELLO (07 04 11 11 14):
 - $(07^{53} \bmod 77)^{37} \bmod 77 = 07$
 - $(04^{53} \bmod 77)^{37} \bmod 77 = 37$
 - $(11^{53} \bmod 77)^{37} \bmod 77 = 44$
 - $(11^{53} \bmod 77)^{37} \bmod 77 = 44$
 - $(14^{53} \bmod 77)^{37} \bmod 77 = 14$
- Alice sends 07 37 44 44 14

Acknowledgements

- Substantial portions of these slides are ©2002-2004 Matt Bishop and used with permission