Announcements

- Exam 2 this week
  - Cheat Sheet due @ midnight tonight
  - Exam 2 available on onCourse @ 8:00 am tomorrow
  - Remember Reference Sheet & Honor Code pledge
  - Major emphasis in grading (and the course!) is quality of explanation of solutions
- This week's Jamboards due on Sunday
- No Problem Set next week
- Advanced Crypto in the spring!
- Coming Attractions this afternoon @ 3:30

Few notes on p and α in DHKE

- Trusted source picks large prime p and $\alpha \in \mathbb{Z}_p^*$ where ord(α) is a large prime

  We saw last week how to construct α from a generator of $\mathbb{Z}_p^*$

- This means $\phi(p) = p - 1$ should have a large prime factor

- Why?
  - Security of DHKE depends upon the DLP $\alpha^x \equiv A \mod p$ being hard to solve
  - Pohlig-Hellman algorithm provides way to solve the DLP based on the factors of ord(α)
  - If ord(α) factors into small values, then computationally feasible to solve this DLP

Quick review

AES

- Secure, efficient symmetric encryption for data/messages
- Requires both parties to have same shared, private key

RSA

- Public key encryption whose security depends upon difficulty of factoring very large numbers
- Use for encrypting data/messages, key exchange, and digital signatures

Diffie-Hellman Key Exchange

- Public key whose security depends on DLP
- Only used for key exchange, not data/message encryption
- Both parties contribute to private key

Comparing Security Levels

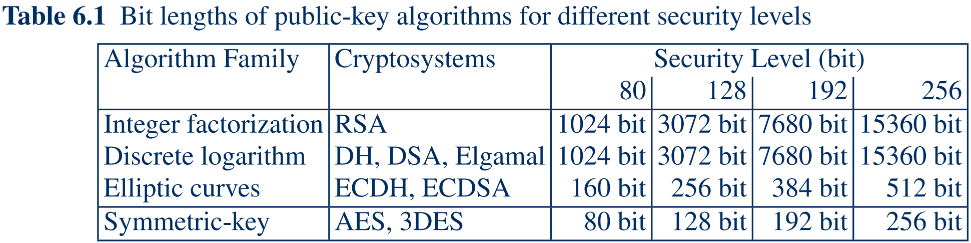

Table 6.1 Bit lengths of public-key algorithms for different security levels

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete logarithm	DH, DSA, Elgamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric-key	AES, 3DES	80 bit	128 bit	192 bit	256 bit

Some desirable properties of a cryptographic system

- **Confidentiality:** Information is kept secret from all but authorized parties
- **Integrity:** Messages have not been modified in transit
- **Message Authentication:** The sender of the message is authentic
- **Nonrepudiation:** The sender cannot deny the creation of the message

Elgamal digital signatures

Key Creation

- Trusted party publishes p and α as in DHKE
- Alice picks private d, publishes public $\beta \equiv \alpha^d \mod p$

Alice signs message x

- Choose ephemeral k_E where $\gcd(k_E, p-1) = 1$
- Computes $r = \alpha^{k_E} \mod p$ and $s \equiv (x - d \cdot r){k_E}^{-1} \mod p-1$
- Sends $(x, (r, s))$

Bob verifies signature

- Computes $t \equiv \beta^r r^s \mod p$
- If $t \equiv \alpha^x \mod p$ then valid signature
  If $t \not\equiv \alpha^x \mod p$ then invalid signature