Other Public-Key Cryptosystems

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

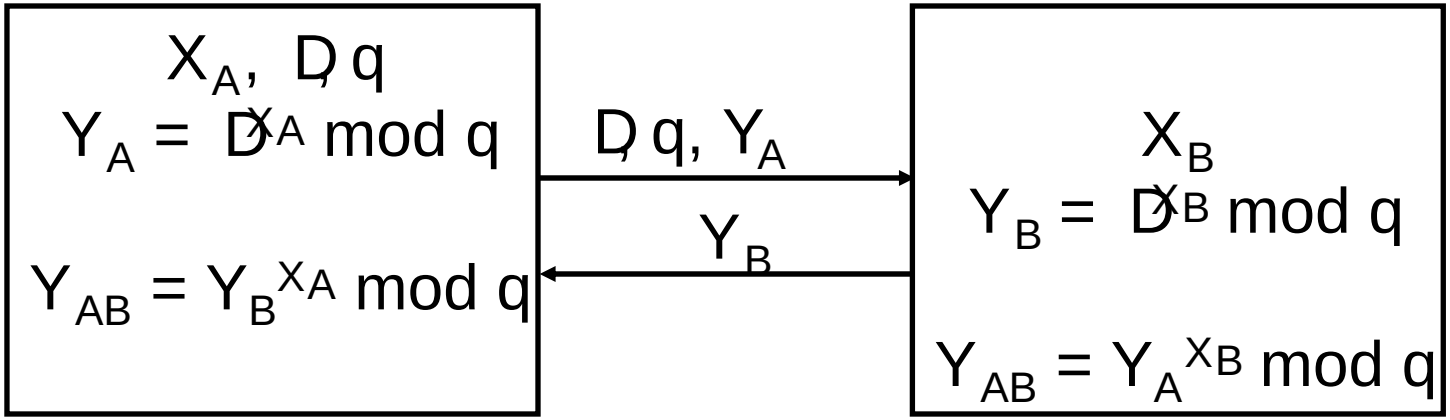
http://www.cse.wustl.edu/~jain/cse571-14/

1. Diffie-Hellman Key Exchange
2. ElGamal Cryptosystem
3. Elliptic Curve Arithmetic
4. Elliptic Curve Cryptography
5. Pseudorandom Number Generation using Asymmetric Cipher

These slides are based partly on Lawrie Brown's slides supplied with William Stallings's book "Cryptography and Network Security: Principles and Practice," 6th Ed, 2013.

Diffie-Hellman Key Agreement

- Allows two party to agree on a secret key using a public channel
- A selects q=large prime, and α=a primitive root of q
- A selects a random X_A, B selects another random X_B



$$Y_{AB} = \alpha^{X_A X_B} \bmod q$$

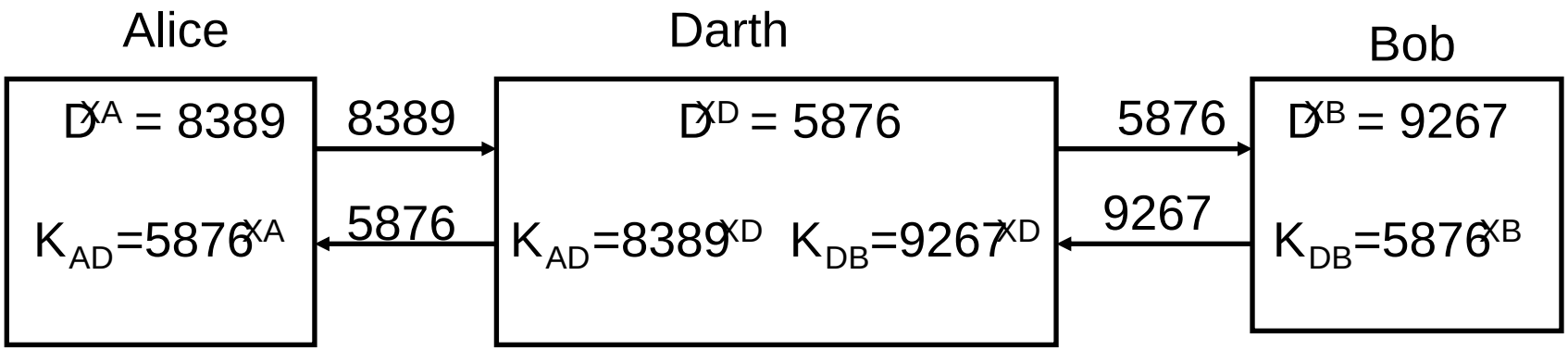
- Eavesdropper can see Y_A, α, q but cannot compute X_A
- Computing X_A requires discrete logarithm - a difficult problem

Diffie-Hellman (Cont)

- Example: a=5, q=19
  - A selects 6 and sends $5^6 \bmod 19 = 7$
  - B selects 7 and sends $5^7 \bmod 19 = 16$
  - A computes $K = 16^6 \bmod 19 = 7$
  - B computes $K = 7^7 \bmod 19 = 7$
- Preferably (q-1)/2 should also be a prime.
- Such primes are called safe prime.

Man-in-Middle Attack on Diffie -Hellman

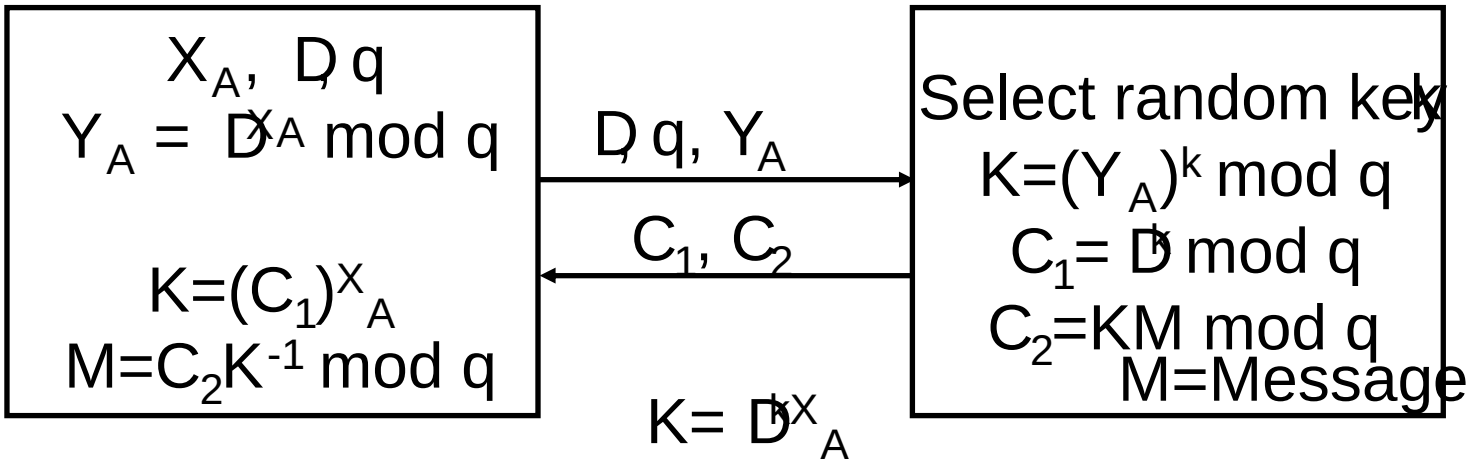
- Diffie-Hellman does not provide authentication



- X can then intercept, decrypt, encrypt, forward all messages between Alice & Bob
- You can use RSA authentication and other alternatives

ElGamal Cryptography

- Public-key cryptosystem related to D-H
- Uses exponentiation in a finite (Galois)
- Security based difficulty of computing discrete logarithms
- X_A is the private key, $\{D, q, Y_A\}$ is the public key

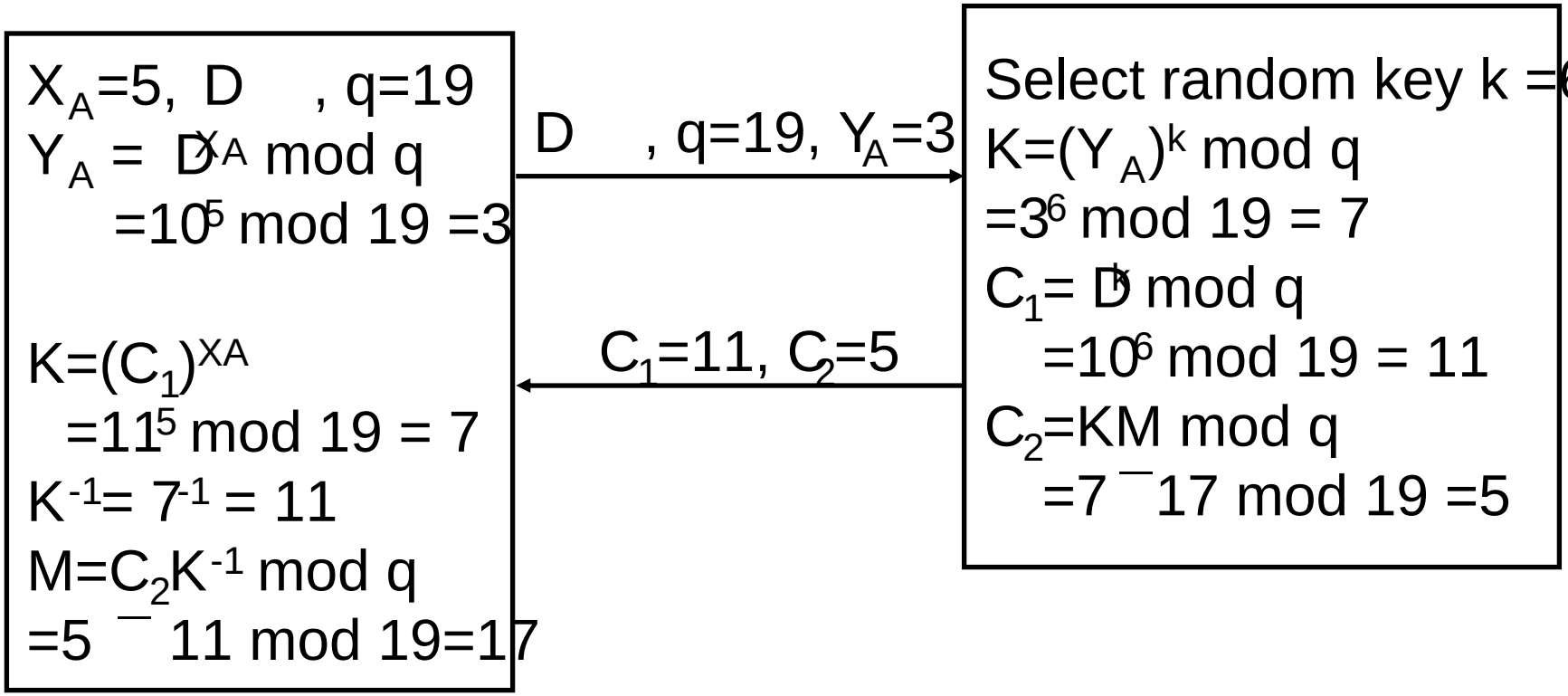


- k must be unique each time. Otherwise insecure.

Ref: http://en.wikipedia.org/wiki/ElGamal_encryption

ElGamal Cryptography Example

- Use field GF(19) q=19 and D=10
- Alice chooses x_A=5,
- Bob wants to sent message M=17, selects a random key k=6



Elliptic Curve Cryptography

- Majority of public-key crypto (RSA, D-H) use either integer or polynomial arithmetic with very large numbers/polynomials
- Imposes a significant load in storing and processing keys and messages
- An alternative is to use elliptic curves
- Offers same security with smaller bit sizes
- Newer, but not as well analyzed

Elliptic Curves over Real Numbers

- An elliptic curve is defined by an equation in two variables x & y,
  - $y^2 = x^3 + ax + b$
  - Where x, y, a, b are all real numbers
  - $4a^3+27b^2 \neq 0$
- The set of points E(a, b) forms an abelian group with respect to "addition" operation defined as follows:
  - P+Q is reflection of the intersection R
  - O (Infinity) acts as additive identity
  - To double a point P, find intersection of tangent and curve
  - Closure: P+Q∈E
  - Associativity: P+(Q+R) = (P+Q)+R
  - Identity: P+O=P
  - Inverse: -P∈E
  - Commutative: P+Q = Q+P

Elliptic Curve over Real Numbers (Cont)

- Slope of line PQ is:
  - $' = (y_Q-y_P)/(x_Q-x_P)$
- The sum R=P+Q is:
  - $x_R= '^2-x_P-x_Q$
  - $y_R=-y_p+ '(x_P-x_R)$
- P+P=2P=R

$$x_R = \left(\frac{3x_P^2 + a}{2y_P}\right)^2 - 2x_P$$

$$y_r = \frac{3x_P^2 + a}{2y_P}(x_P - x_R) - y_P$$