Asymmetric Key Cryptography

Overview and Description of RSA, El Gamal, and Elliptic Curve Crypto

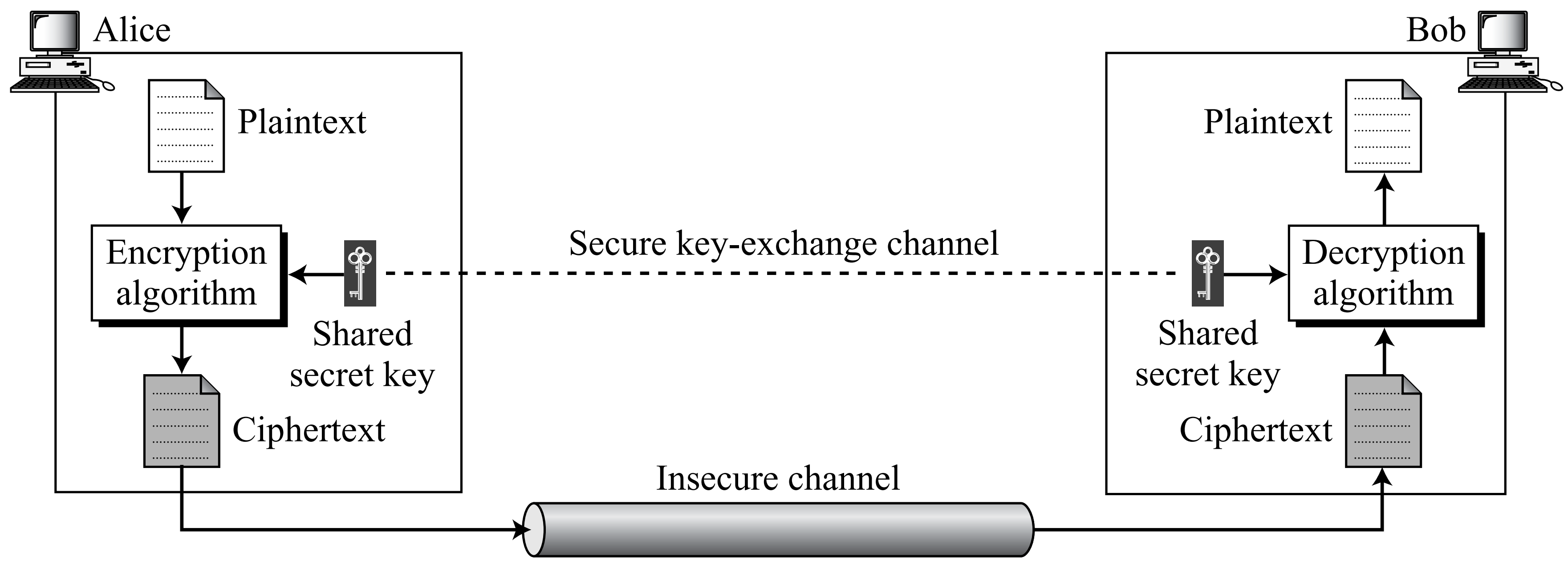
Priyank Kalla

Professor

Electrical & Computer Engineering

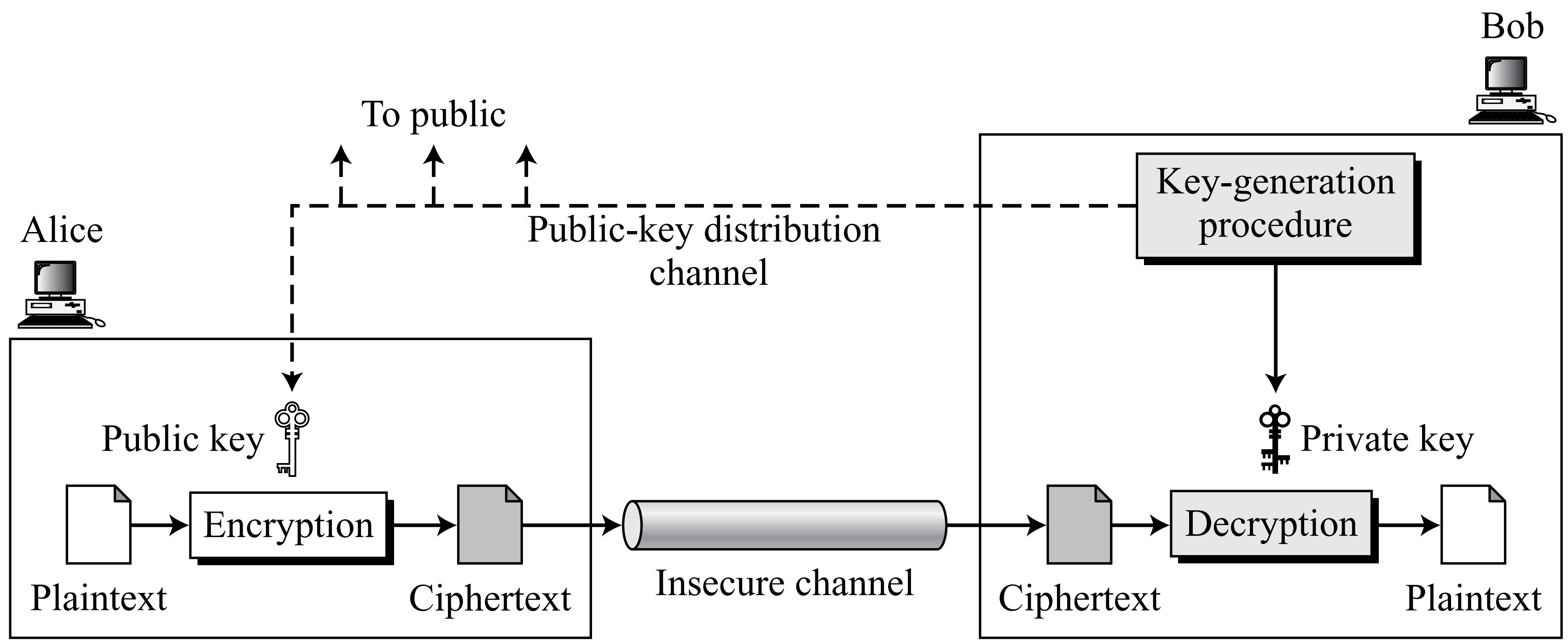
THE UNIVERSITY OF UTAH

Recall: Symmetric Key Crypto



- Plaintext P, Ciphertext C, key k, Encryption algorithm $E_k(P)$, Decryption algorithm $D_k(C)$
  - $C = E_k(P), \quad D_k(C) = P$
  - $D_k(E_k(x)) = E_k(D_k(x)) = x$: Encryption/Decryption are inverses of each other
- Need a "secure" key exchange mechanism — will study later
- **Symmetric**: same key for E_k, D_k and also for two-way communication between Alice $\Longleftrightarrow$Bob
- Need a separate key for each channel
- Key is the secret, E_k, D_k may be known to the public (adversary): Kerchoff's principle

Asymmetric Key Crypto



- The receiver Bob broadcasts a “public key” to everyone
- If number of senders to Bob = n, still Bob broadcasts only 1 public key
- Each receiver has to generate a public key
- Bob also generates a private key, related to the public key
- Alice encrypts using Bob’s public key, Bob decrypts using his private key
- Public key = lock, private key = unlock

Symmetric vs Asymmetric

- Symmetric: Secret (key) must be shared
  - In a community of n people, $n(n-1)/2$ public keys needed
- Asymmetric: The secret is personal
  - Preferable, but computationally much harder
  - Between n people, only n keys are needed, 1 for each receiver
- For large data sets (files), symmetric crypto is used (AES)
- For small data-sets, for key exchanges and for message authentication (digital signatures), asymmetric crypto makes sense
- Symmetric and asymmetric crypto complement each other
- In asymmetric crypto: messages and keys = bit-vectors = numbers (integers or finite field elements). No permutations!

Symmetric vs Asymmetric

- Examples of Asymmetric Key Ciphers: Knapsack crypto system, McEliece system, RSA, Rabin, El Gamal, Elliptic Curve Cryptosystem (ECC)

- We will take a look at: RSA, El Gamal and ECC

- Asymmetric crypto systems rely on Trapdoor One-Way Functions (TOWF)

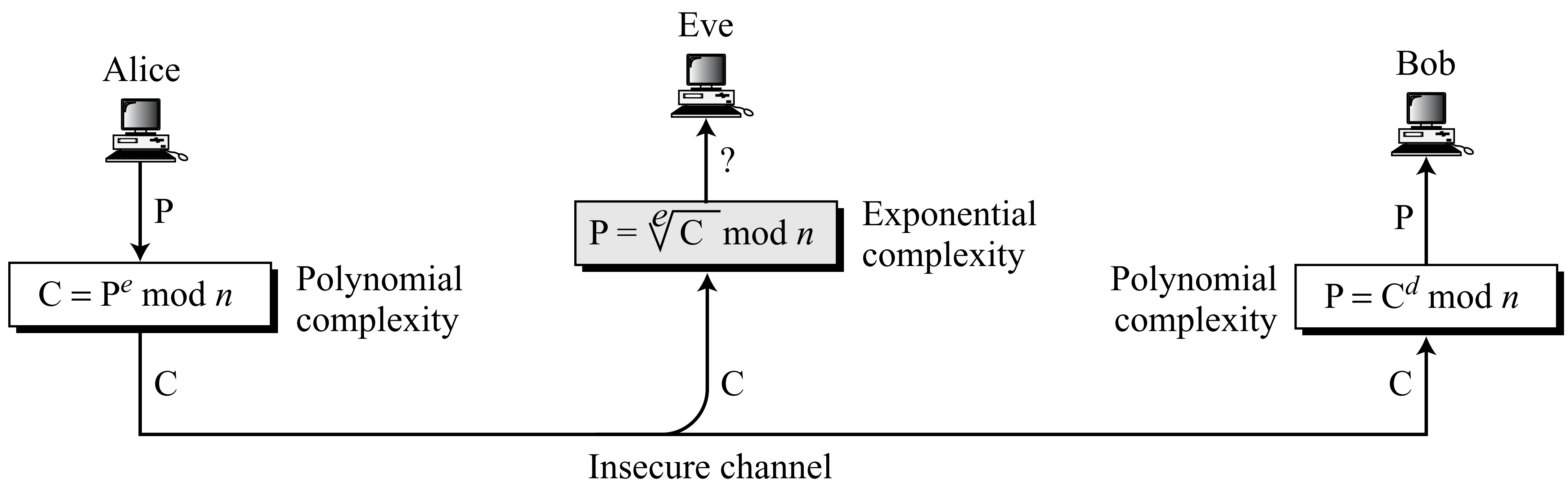
  - Given $x, y = f(x)$ is easy to compute (Encryption is easy)

  - But, $x = f^{-1}(y)$ is computationally infeasible (Cannot break the system security)

  - Moreover, given a trapdoor secret, $x = f^{-1}$ can be computed (Decryption is easy to compute)

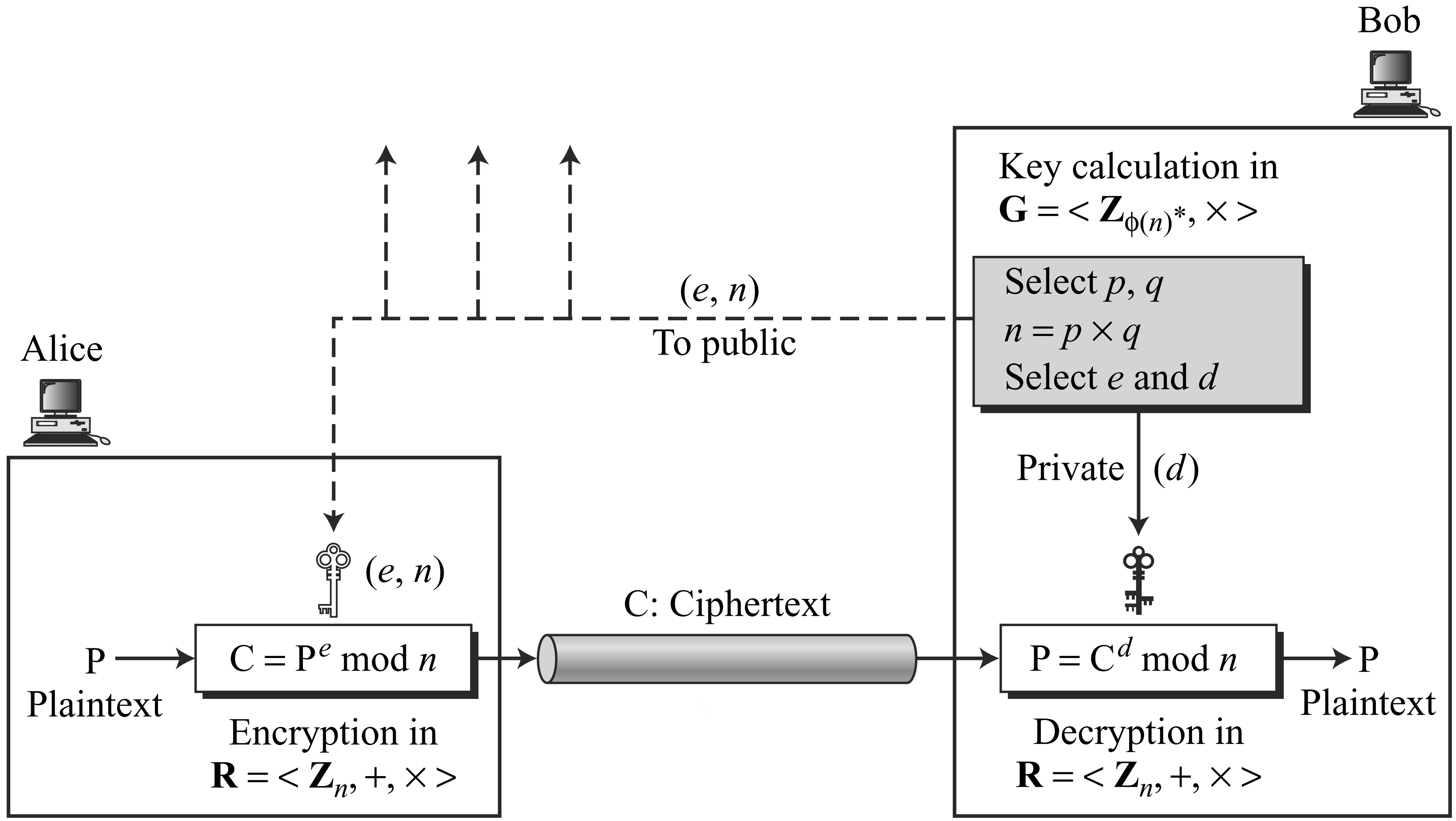
- These systems rely on the infeasibility of "integer modular factorization" problem (RSA), or "discrete logarithm problem" (El Gamal), or "elliptic curve logarithm problem" (ECC), for large key sizes

Rivest Shamir Adleman (RSA)



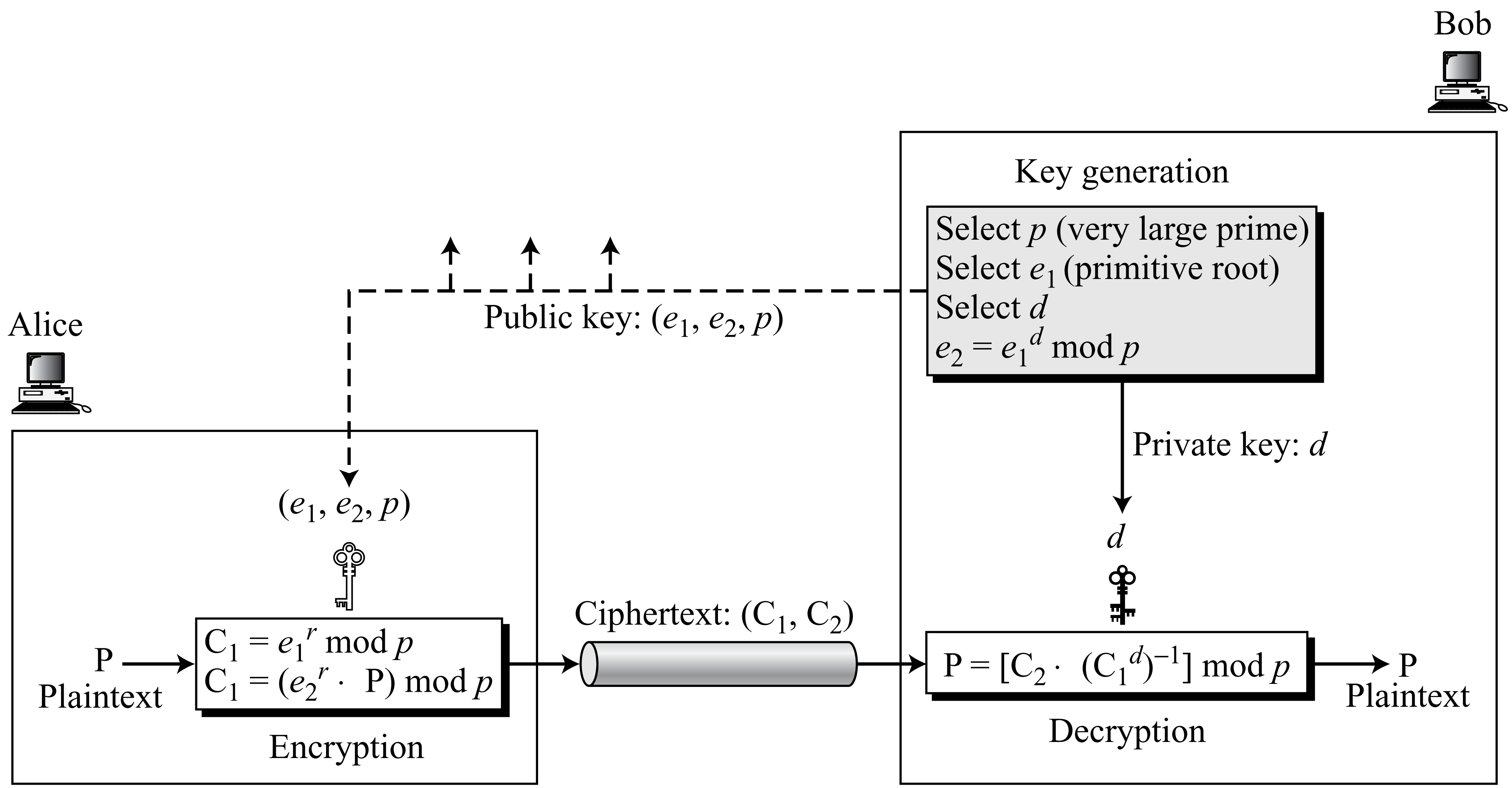
- Two algebraic objects: 1) Integer ring $(\mathrm{mod}\ n) = (\mathbb{Z}_n, +, \times)$, and 2) multiplicative group $G = (\mathbb{Z}^*_{\phi(n)}, \times)$
- We'll study $G = (\mathbb{Z}^*_{\phi(n)}, \times)$ in more detail shortly
- $\phi(n) =$ Euler's totient function or Euler's phi function = the number of integers less than n that are relatively prime to n
- Modular logarithm (Eve) is as hard as factoring the modulus (exponential) complexity
- For large n = 300 decimal digits = 1024 bits, system is fairly secure
- 1024-bit modulo multiplier circuit is not feasible: mostly software crypto system

Rivest Shamir Adleman (RSA)



- $p, q =$ large prime numbers, $n = p \times q$, $\phi(n) = (p-1)(q-1)$
- Select $e < \phi(n)$, such that e and $\phi(n)$ are coprime
- $d = e^{-1} \pmod{\phi(n)}$
- Public key (e, n), Bob's private key = d

El Gamal

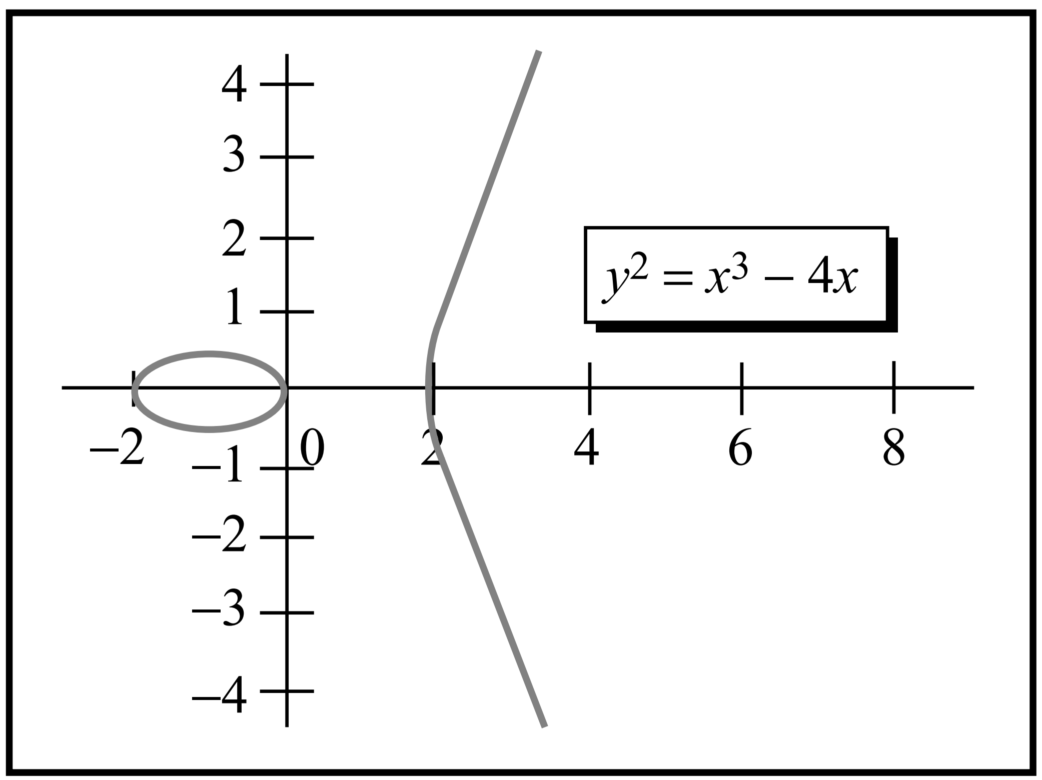


- El Gamal uses the field $\mathbb{F}_p = (\mathbb{Z}_p, + , \times)$, and the group $G = (\mathbb{Z}_p^*, \times)$ for computations
- Security relies on the complexity of the discrete logarithm problem:
  $r = \log_{e_1} e_2 \pmod p$ is infeasible for a large prime p = 1024 bits large
- Alice's $r =$ random number

Elliptic Curve Crypto

- General equation for elliptic curve:
$y^2 + b_1xy + b_2y = x^3 + a_1x^2 + a_2x + a_3$

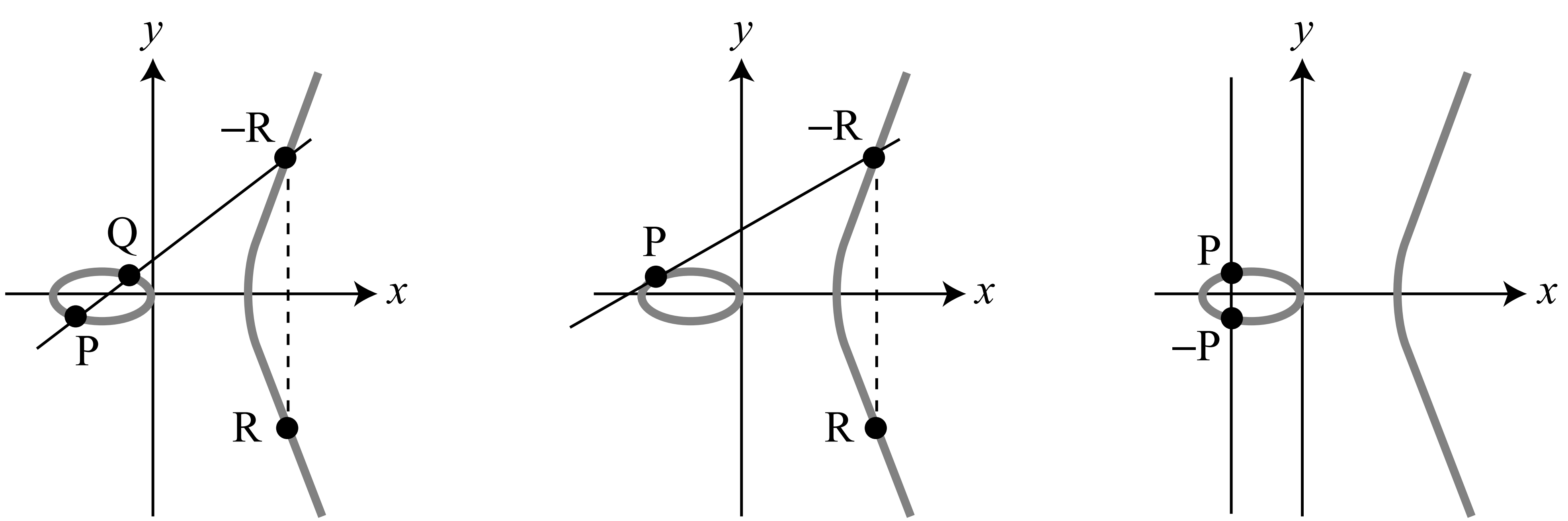
- Over real numbers, for example, $y^2 = x^3 - 4x$



a. Three real roots

Elliptic Curve Crypto

- Encipherment depends upon point multiplications, point additions and point inverses
- Multiplication = repeated addition
- Curves are usually defined over finite fields. Points on curves form a group
- O = P + (-P) = additive identity of the group



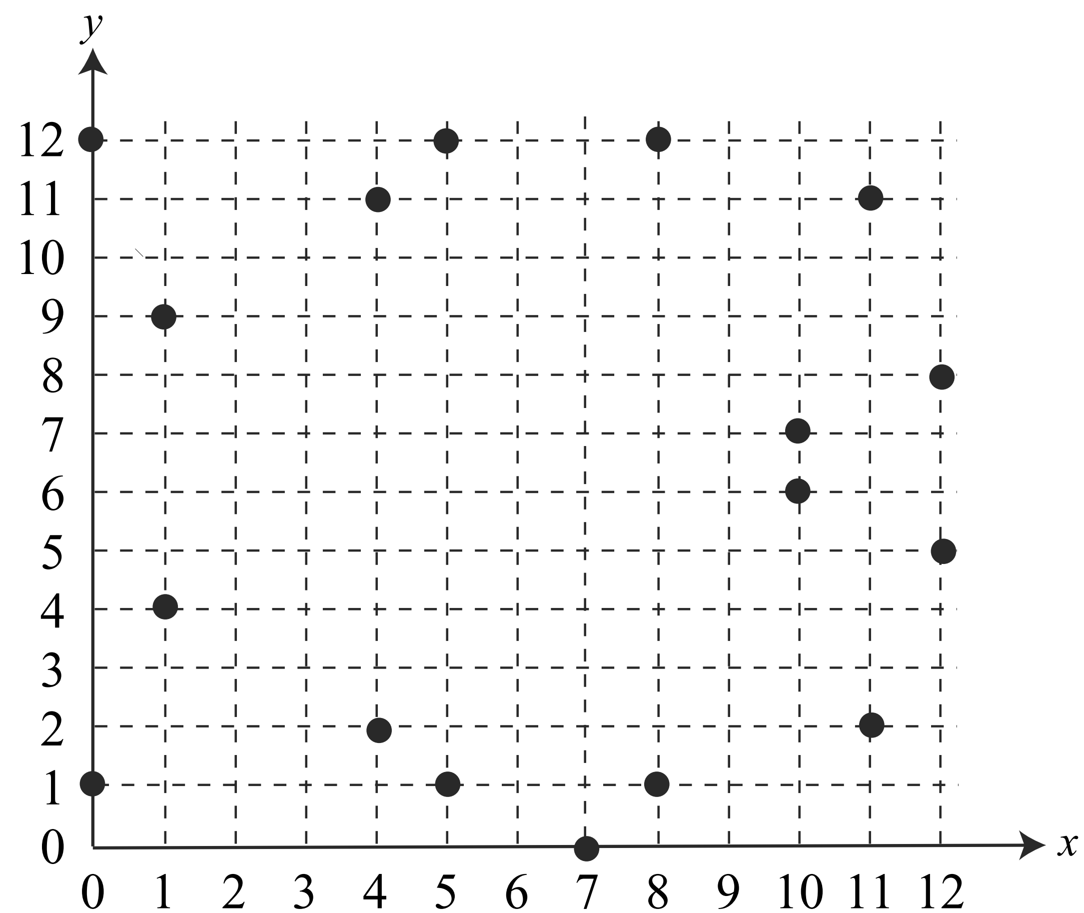
a. (R = P + Q)　　b. (R = P + P)　　c. (O = P + (– P))

Points on Elliptic Curves

- Example: $\mathbb{F}_{13} = \mathbb{Z}_{13} : y^2 = x^3 + x + 1 \pmod{13}$

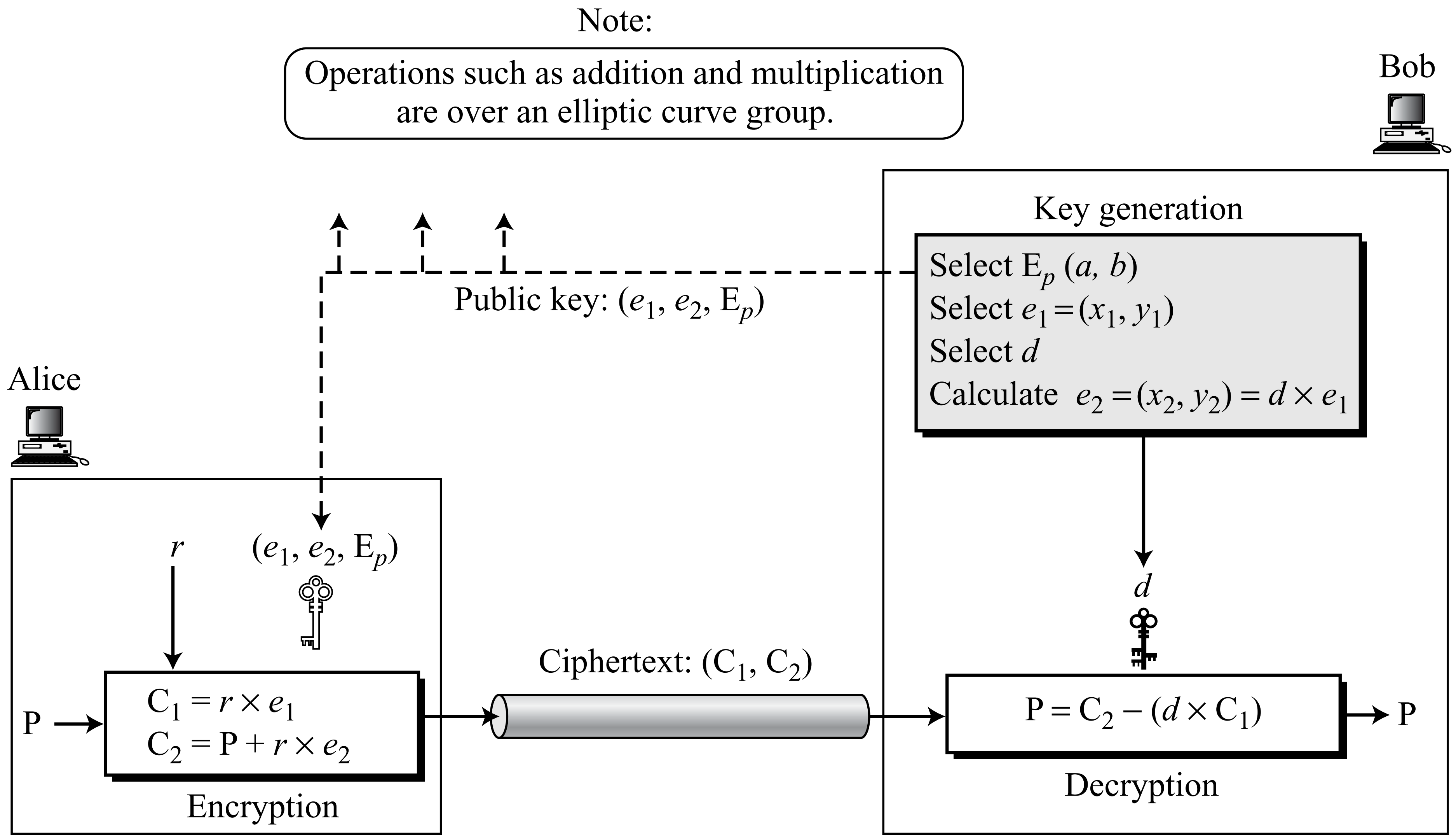
(0, 1)	(0, 12)
(1, 4)	(1, 9)
(4, 2)	(4, 11)
(5, 1)	(5, 12)
(7, 0)	(7, 0)
(8, 1)	(8, 12)
(10, 6)	(10, 7)
(11, 2)	(11, 11)
(12, 5)	(12, 8)

Points



Graph

El Gamal over Elliptic Curve



- Security: 160-bits of ECC gives the similar security as 1024 bits of RSA

Math for RSA: prime numbers and Euler's totient

- $p =$ prime, $n =$ integer, $\mathbb{Z}_n^* =$ set of integers less than n that are relatively prime to n
- Euler's totient function $\phi(n) =$ number of integers relatively prime to n = $|\mathbb{Z}_n^*|$
- Calculation:
  - $\phi(1) = 0$
  - $\phi(p) = p - 1, p =$ prime
  - $\phi(m \times n) = \phi(m) \times \phi(n),$ if n, m are relatively prime
  - $\phi(p^e) = p^e - p^{e-1}, p =$ prime

Examples $\phi(n)$ Computation

- $\phi(13) = (13 - 1) = 12.$
- $\phi(10) = \phi(2) \times \phi(5) = 1 \times 4 = 4,$
- $240 = 2^4 \times 3^1 \times 5^1.$
- $\phi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0) = 64$
- $\phi(49) = 7^2 - 7^1 = 42.$