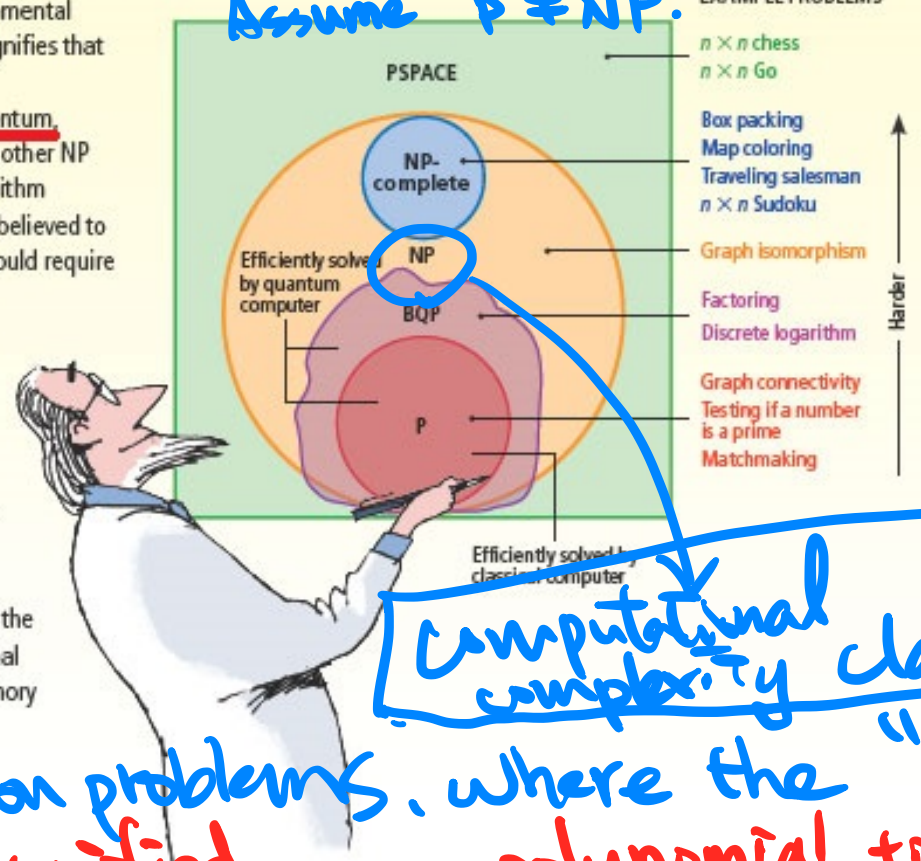
Where Quantum Computers Fit In

The map at the right depicts how the class of problems that quantum computers would solve efficiently (BQP) might relate to other fundamental classes of computational problems. (The irregular border signifies that BQP does not seem to fit neatly with the other classes.)

The BQP class (the letters stand for *bounded-error, quantum, polynomial time*) includes all the P problems and also a few other NP problems, such as factoring and the so-called discrete logarithm problem. Most other NP and all NP-complete problems are believed to be outside BQP, meaning that even a quantum computer would require more than a polynomial number of steps to solve them.

In addition, BQP might protrude beyond NP, meaning that quantum computers could solve certain problems faster than classical computers could even check the answer. (Recall that a conventional computer can efficiently verify the answer of an NP problem but can efficiently solve only the P problems.) To date, however, no convincing example of such a problem is known.

Computer scientists do know that BQP cannot extend outside the class known as PSPACE, which also contains all the NP problems. PSPACE problems are those that a conventional computer can solve using only a polynomial amount of memory but possibly requiring an exponential number of steps.



$P \subseteq NP$

Assume $P \neq NP$.

Computational complexity classes.

NP: a class of decision problems. where the "Yes" instances can be verified in polynomial time

(Scott Aaronson, *Scientific American* 298, 62 - 69 (2008))

P: a class of decision problems that can be solved in polynomial time

needs $\tilde{O}(2^{0.5n})$ trivially.

① Given an integer $M \in \mathbb{Z}$, whether M is a prime (composite) number or not? (This is an NP problem)

M is a prime if there is no $Q > 1$ such that Q is a divisor of M.

Otherwise, it is a composite number.

Ex. 3, 5, 7, are prime.

$15 = 3 \times 5$ is a composite number.

② Given an integer M, whether $Q \in \mathbb{Z}$ is a factor of M?

(This problem is in P.)

Both problems are decision problems.

Open System Interconnection.

- **Security attack**: Any action that compromises the security of information
- **Security mechanism**: A process that is designed to detect, prevent, or recover from a security attack
- **Security service**: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization

Security attack: Any action that compromises the security of information.

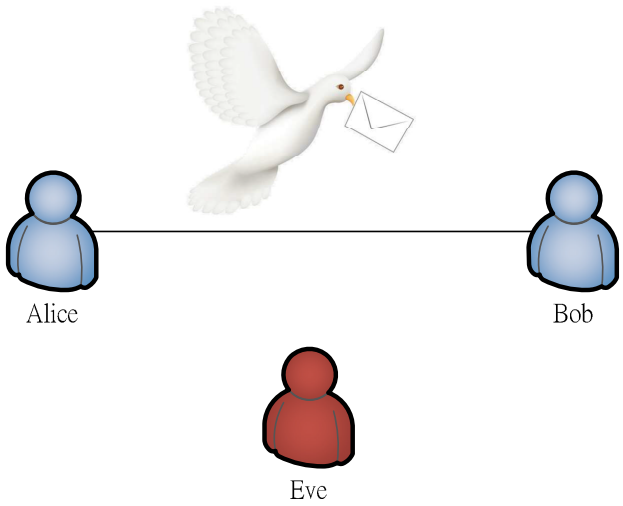
- **passive attack**: to learn or make use of information from the system but does not affect system resources
  - The release of message contents
  - Traffic analysis
- **active attack**: to alter system resources or affect their operation
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of service

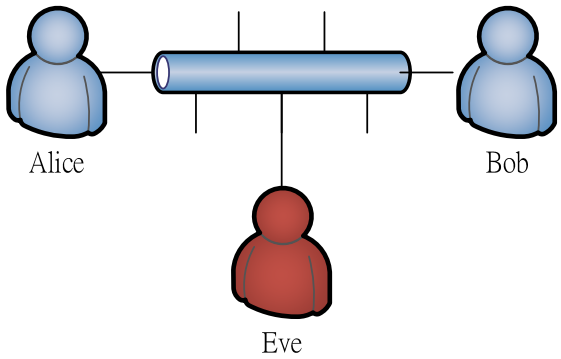
Fig. 1.2

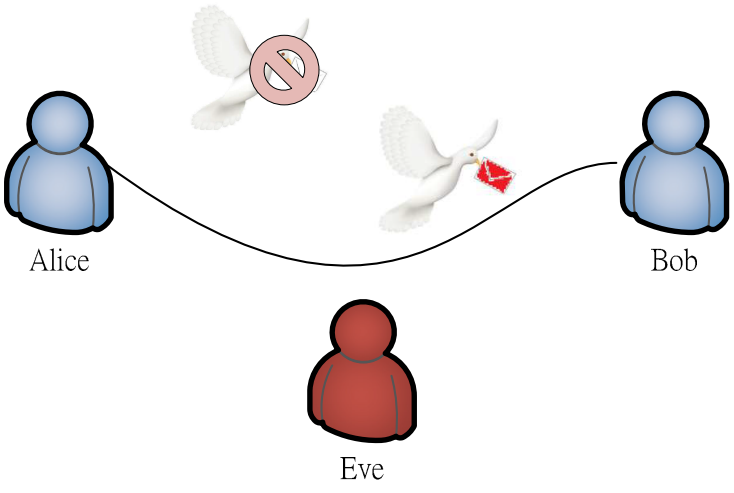
See also Tables 1.2 & 1.3

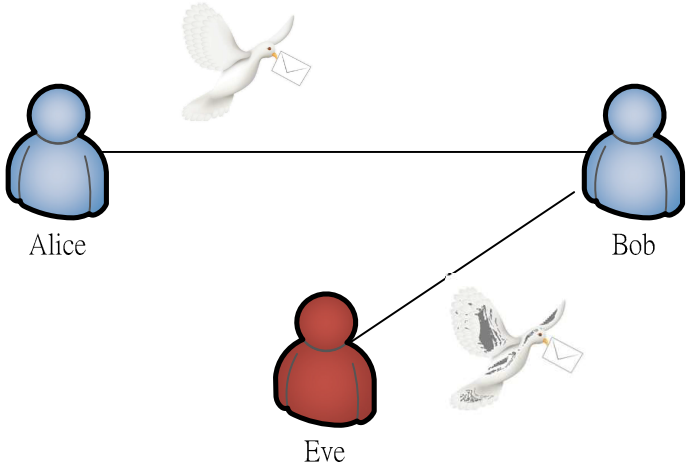
- **Threat**: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
- **Attack**: An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

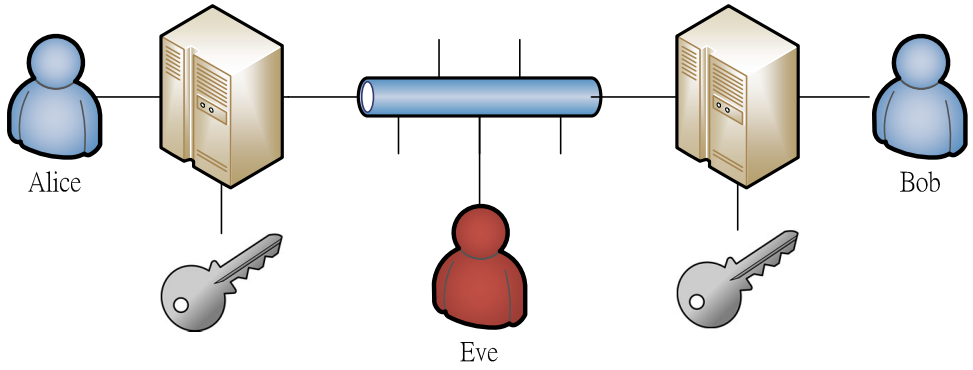
- Symmetric encryption
- Asymmetric encryption
- Data integrity algorithms
- Authentication protocols



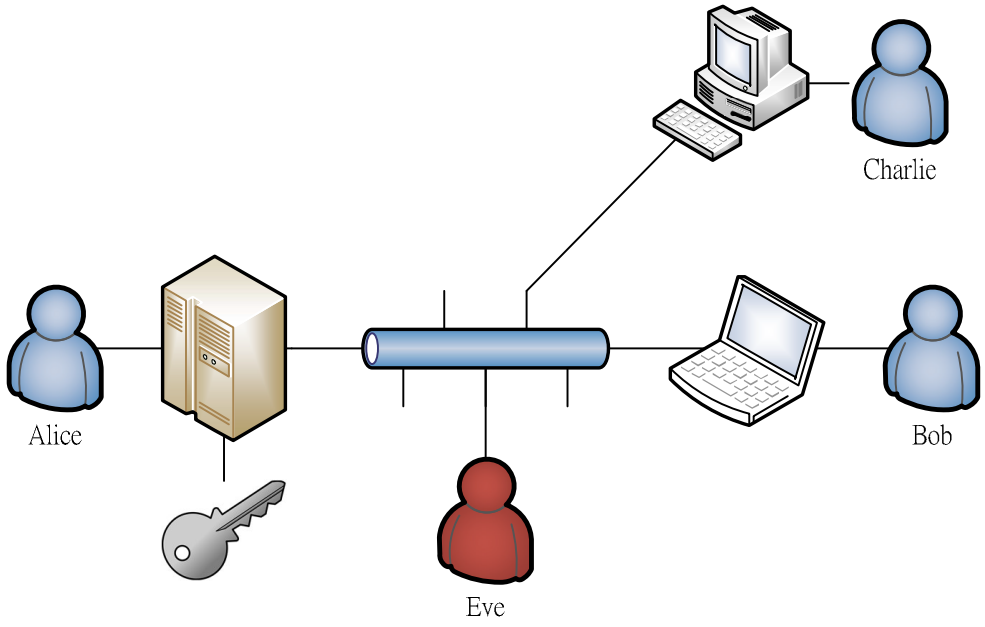



Alice
Bob
Eve


Alice
Bob
Eve



- Example: one-time pad (§3.2).



- Example: RSA (Ron Rivest, Adi Shamir and Leonard Adleman) is an algorithm for public-key cryptography that is based on the presumed difficulty of the factoring problem .
- The largest number that is the product of two large primes of similar size and yet factored is RSA-768, a 768-bit number with 232 decimal digits, on December 12, 2009. It takes almost 2000 years of computing on a single-core 2.2 GHz AMD Opteron. $\sim 10^{20}$ operations