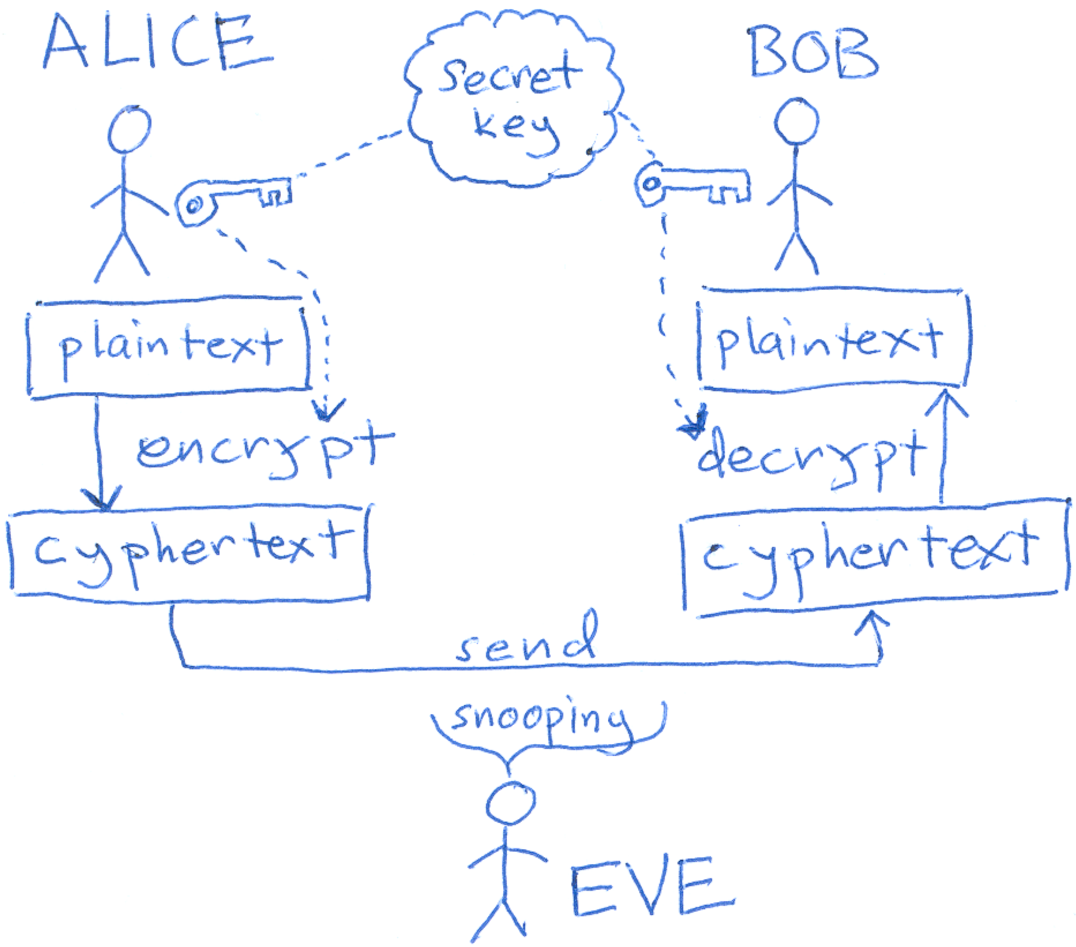
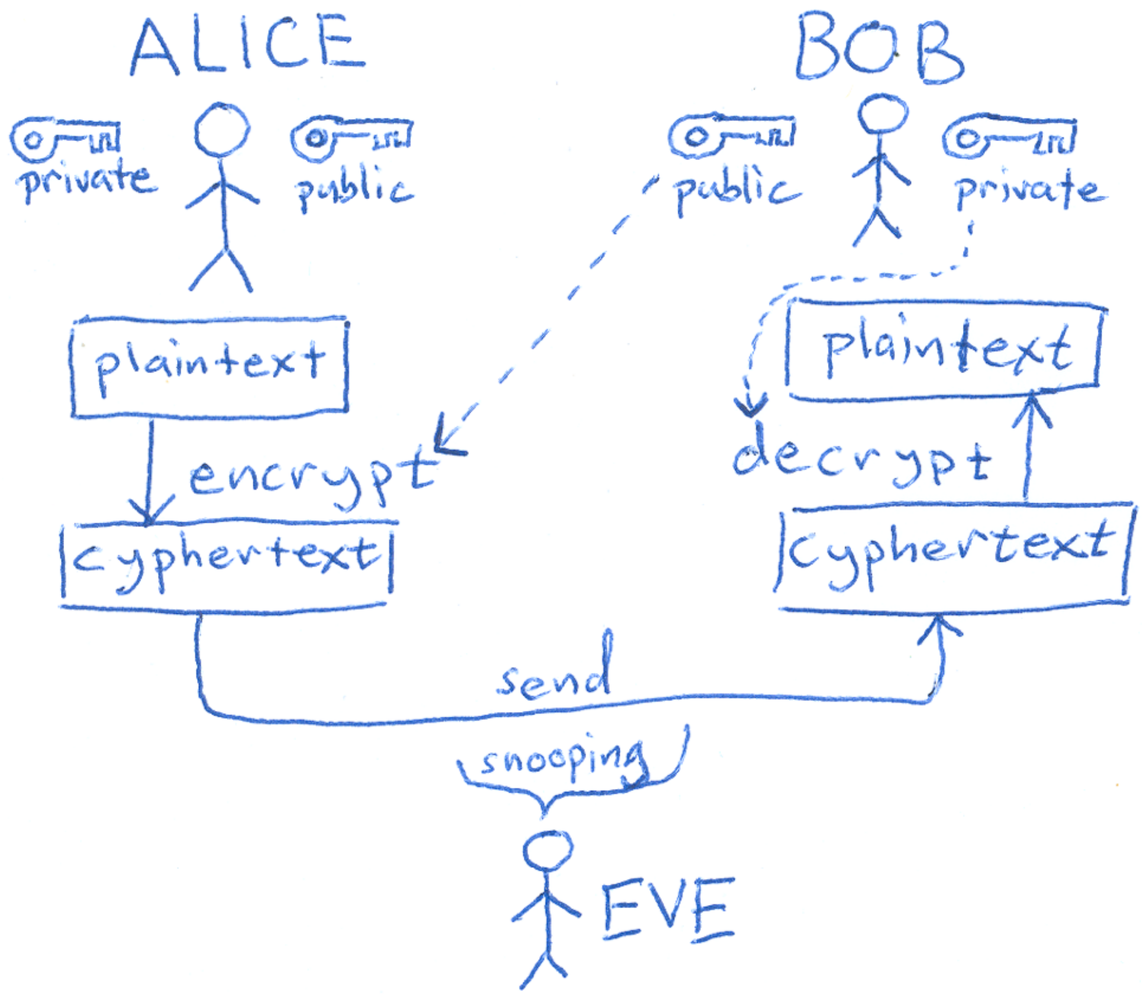
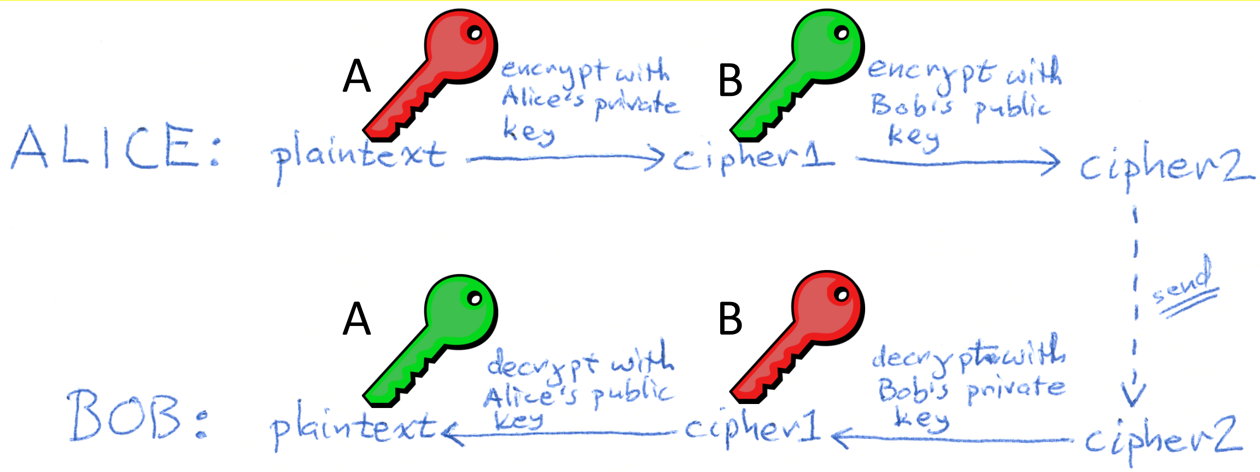
Symmetric Key Encryption



Asymmetric (Public-Key) Encryption



Asymmetric (Public-Key) Encryption with Message Signing



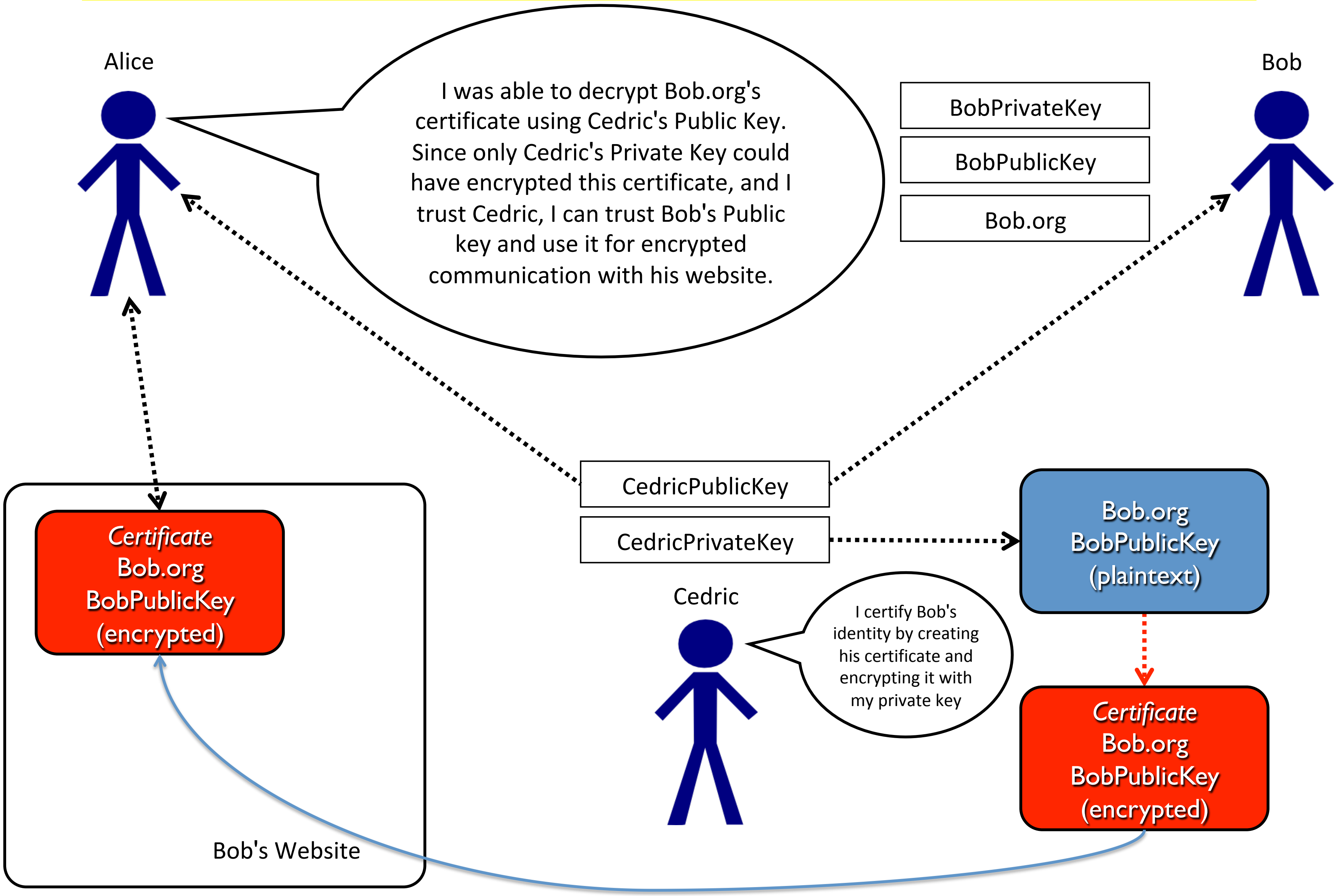
1. Scheme is commutative -- meaning the roles of the public and private keys can be interchanged. Both can either encrypt or decrypt, but once a file is encrypted, ***<u>the same key that encrypted it cannot be used to decrypt it!</u>***

2. If Alice's plaintext message is ***M***, she first encrypts ***M*** with her private key, then with Bob's public key

3. If Bob takes the message he receives and decrypts first with his private key and then with Alice's public key, he'll recover ***M***

4. The guarantees are that <u>only</u> Bob can read the message, and <u>only</u> Alice could have sent it -- ensures <u>confidentially</u> (Alice knows Bob's the only one who can read her message), <u>authentication</u> (Bob knows that Alice sent it) and non-repudiation (Alice can't claim that she didn't sent it)

Trusted Certificates For Website Access



RSA Encryption Scheme

Rivest, Shamir & Adleman

n is the same in both

(e,n) Public Key 2-large integers

(d,n) Private Key 2-large integers

1. The integer ***n*** is the product of two prime numbers, which is called a semi-prime. We say, ***n=pq***, where ***p*** and ***q*** are prime
2. if we know ***e,n,p,q*** then we can calculate d (complex math)
3. The security hinges on ***n*** being <u>really</u> big (usually 2048 bits or greater) and recognizing that factoring really large integers is hard
4. Schemes don't currently exist to factor numbers of that size quickly (within the lifetime of planet earth), so RSA ***seems*** pretty secure
5. Nobody has proved that it's impossible to factor numbers quickly either, so RSA may be broken......................someday