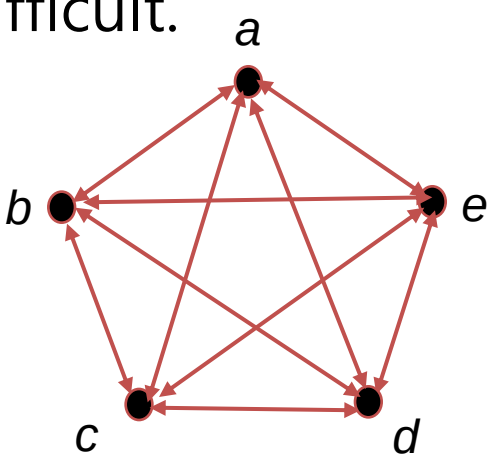
Week 9-1: Public Key Cryptography (PKC)

Problem of Secret key Cryptosystem

- Sharing key in Secret key cryptosystem
  - Given complete graph with n nodes (entities),

    ${}_nC_2 = n(n-1)/2$ pairs secret keys are required.

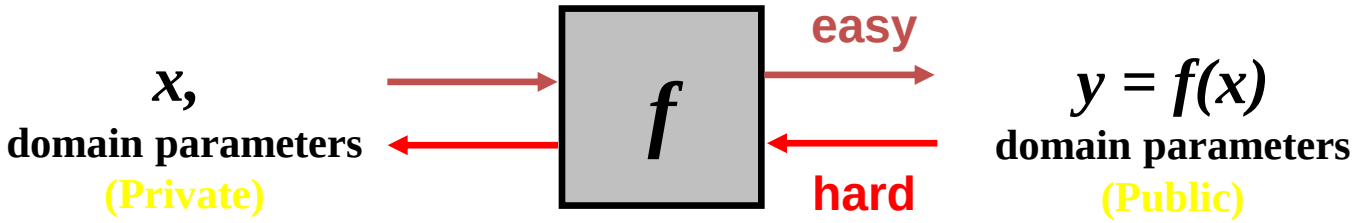
    (Ex.) If n=100, 99 x 50 = 4,950 keys
  - Problem: Managing large number of secret keys is difficult.



Secret keys are required between
(a,b), (a,c), (a,d), (a,e), (b,c),
(b,d), (b,e), (c,d), (c,e), (d,e)

Public Key Cryptography
: key agreement with one-way function

- One-way function
  - Given *x*, easy to compute *y=f(x).*
  - Difficult to compute $x=f^{-1}(y)$ for given *y.*



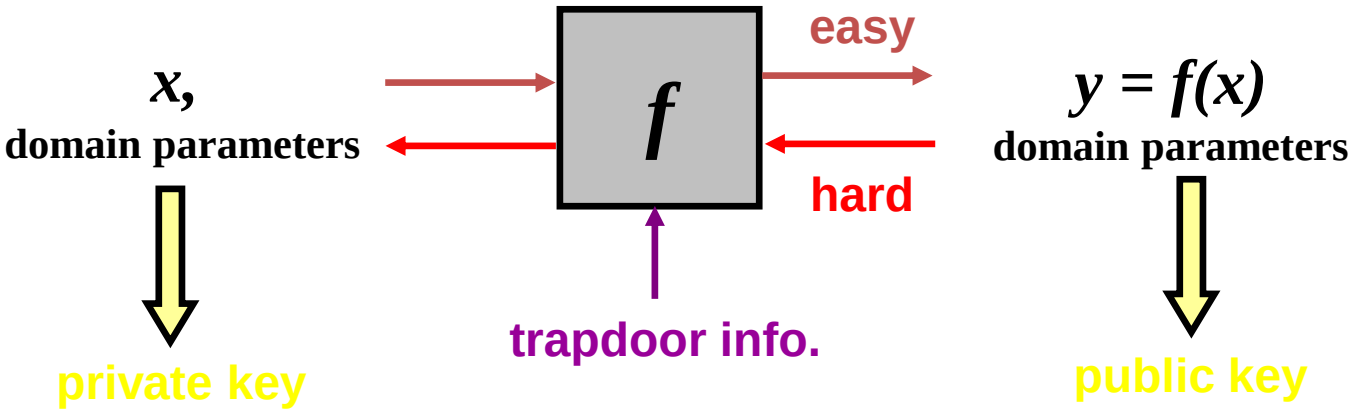
Ex) $f(x)= 7x^{21} + 3x^3 + 13x^2+1 \bmod (2^{15}-1)$

- **DH key Agreement**

  Diffie and Hellman, "*New directions in Cryptography*", IEEE Tr. on IT. ,Vol. 22, pp. 644-654, Nov., 1976.

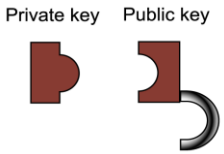
Public Key Cryptography
: Trapdoor one-way function

- Given *x*, easy to compute *f(x)*
- Given *y*, difficult to compute $f^{-1}(y)$ in general
- Easy to compute $f^{-1}(y)$ for given *y* to only who knows certain information (which we call trapdoor information)
- Mathematical Hard Problems

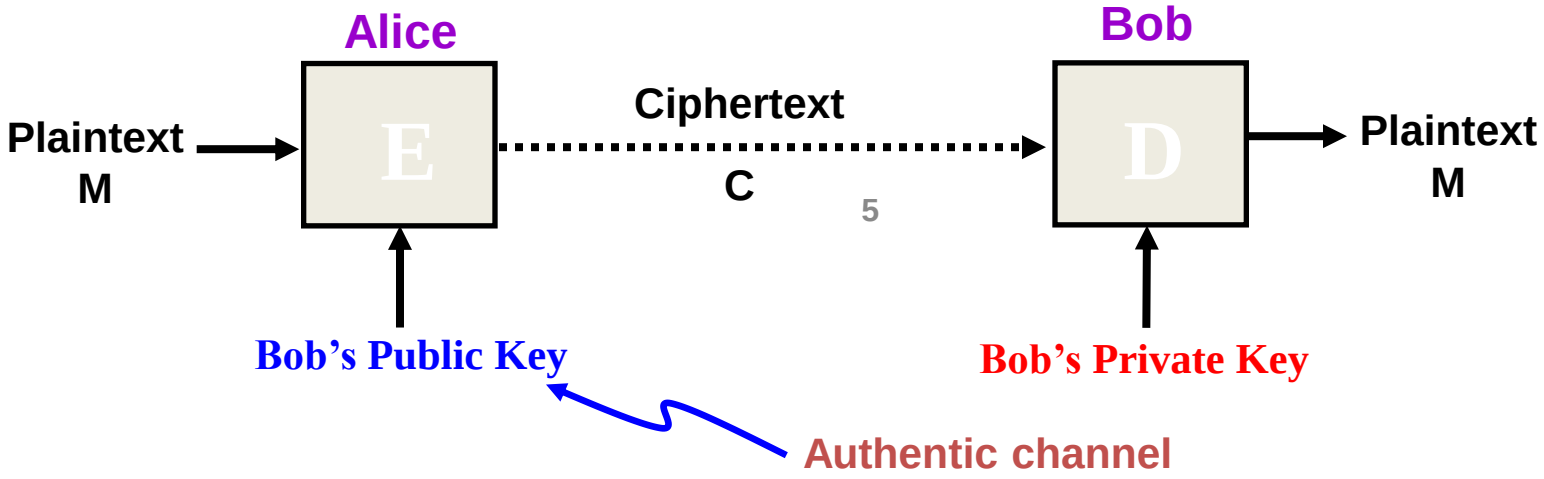


But, easy if trapdoor info. is given.

PKC - Overview (1/3)

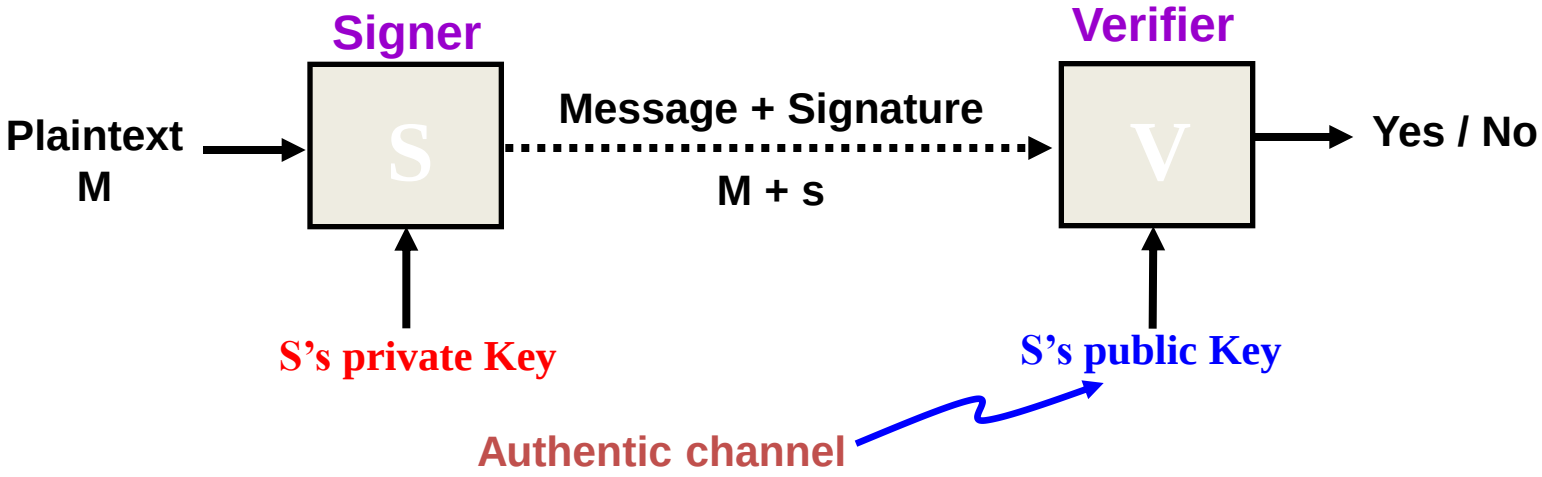


- Using trapdoor 1-way functions,
  - Each user needs to keep securely only his private key.
  - All public keys of users are published.
  - {Asymmetric, 2-keys or Public Key} Cryptosystem
- Privacy (Encryption)
  - Anyone can lock using B's public key
  - Only the receiver can unlock using B's private key



PKC-Overview (2/3)

- Authentication (Digital Signature)
  - Only the signer can sign using S's private key
  - Any Verifier can verify using S's public key



PKC - Overview(3/3)

- Encryption schemes
  - RSA: based on IFP
  - ElGamal: based on DLP
- Digital Signature schemes
  - Signature schemes with message recovery: RSA, etc
  - Signature with appendix: ElGamal, DSA, KCDSA, etc
- Key exchange schemes
  - Key transport: TA(Trusted Authority) generates and distributes key
  - Key agreement: Diffie-Hellman key agreement
- All problems clear?
  - ✓ New Problem : How to get the right peer's Public Key?
  - ✓ Public key infrastructure (PKI) required
  - ✓ Certificate is used to authenticate public key

PKC- History

- RSA scheme (1978)
  - *R.L.Rivest, A.Shamir, L.Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems",CACM, Vol.21, No.2, pp.120-126,Feb,1978*
- McEliece scheme (1978) : Linear coding
- Rabin scheme (1979) : Provable PKC
- Knapsack scheme (1979-): Merkle-Hellman, Chor-Rivest, *etc*.
- ElGamal scheme (1985)
- Elliptic Curve Cryptosystem (1985): Koblitz, Miller
- Non-Abelian group Cryptography (2000): Braid group

Comparison

O : Good X : Bad

	Symmetric	Asymmetric
Key relation	Enc. key = Dec. key	Enc. Key ≠ Dec. key
Enc. Key	Secret	Public, {Private}
Dec. key	Secret	Private, {Public}
Algorithm	Classified Open	Open
Example	SKIPJACK AES	RSA
Key Distribution	Required (X)	Not required (O)
Number of key	Many (X)	Small (O)
Performance	Fast(O)	Slow(X)