Two Cryptography Systems (2)

II. Public-Private Key systems:

- K_{Apriv} = Alice's private key; known only to Alice
- K_{Apub} = Alice's public key; known to *everyone*
- Anything encrypted with K_{Apriv} can be decrypted only with K_{Apub}
- Anything encrypted with K_{Apub} can be decrypted only with K_{Apriv}

•RSA and PGP fall into these category

- RSA = Rivest Shamir Adleman
- PGP = Pretty Good Privacy
- Keys are several 100s or 1000s of b long
- Longer keys => harder for attackers to break
- Public keys maintained via PKI (Public Key Infrastructure)