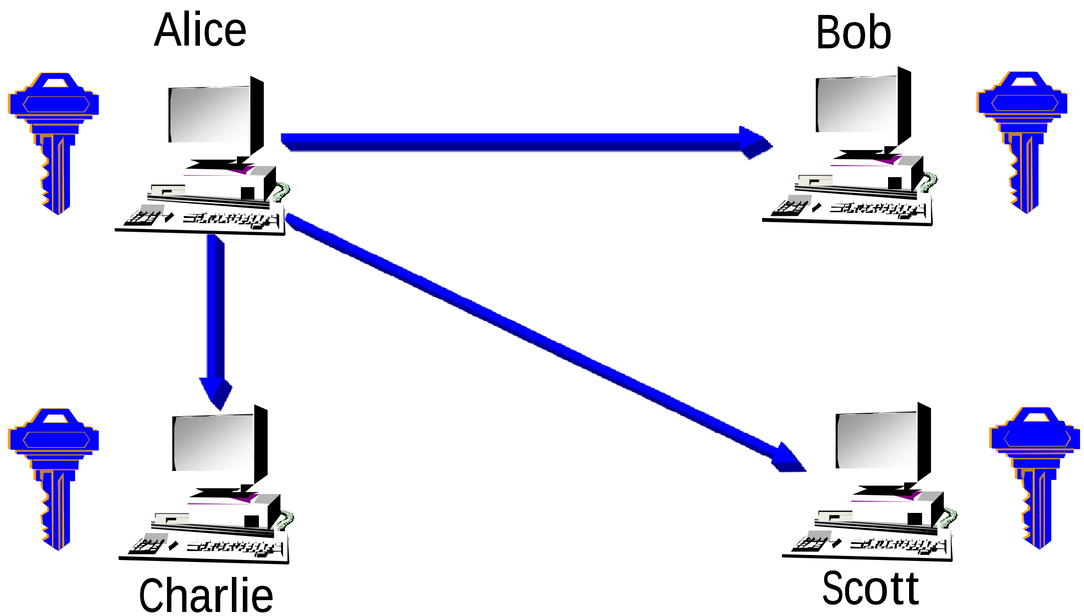
WEP Attacks

- Initial connection sniffing
- IV Reuse
  - Look for IV collisions
  - Some APs reset IV to 0 each time system is (re)initialized
  - IV Dictionary Attacks
- Injection attacks with known plaintext
- Wi-fi Protected Access / 802.11i

IV Reuse Occurrences

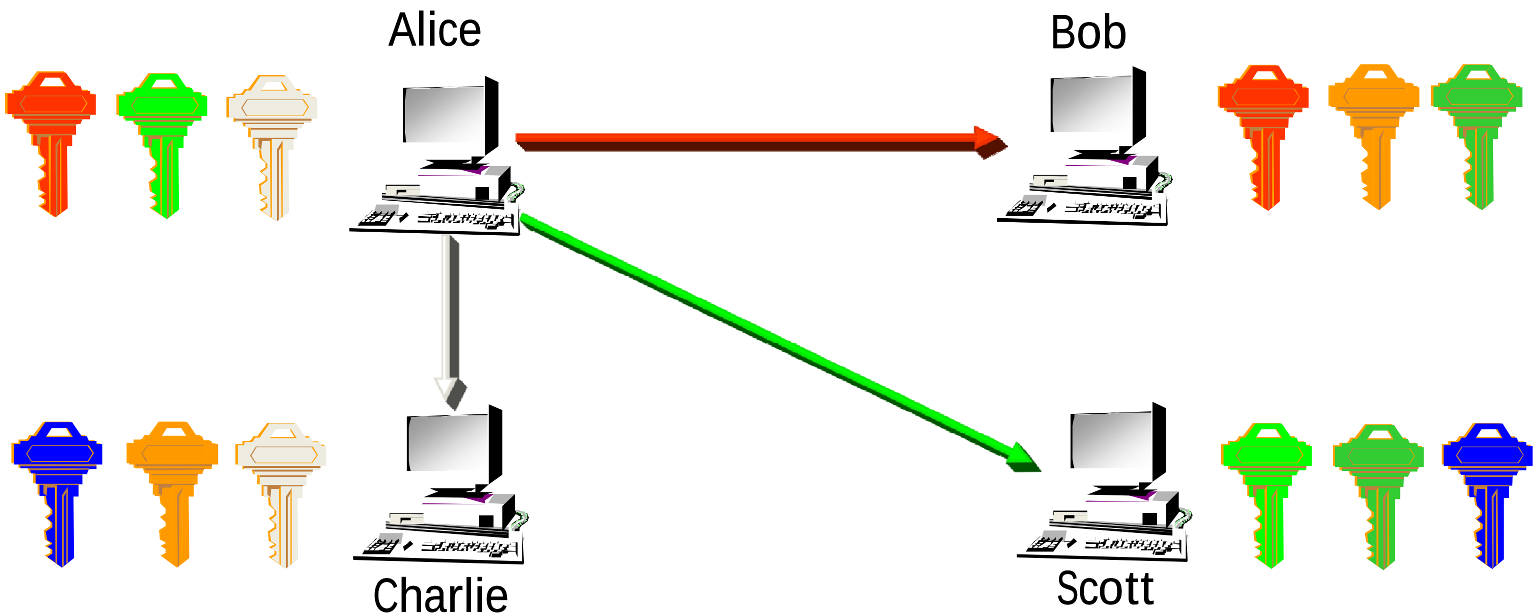
- 1% after 582 encrypted frames
- 10% after 1,881 encrypted frames
- 50% after 4,823 encrypted frames
- 99% after 12,430 encrypted frames

Shared Secret Key Distribution



- How does Alice distribute the key?
- What happens if Scott leaves?

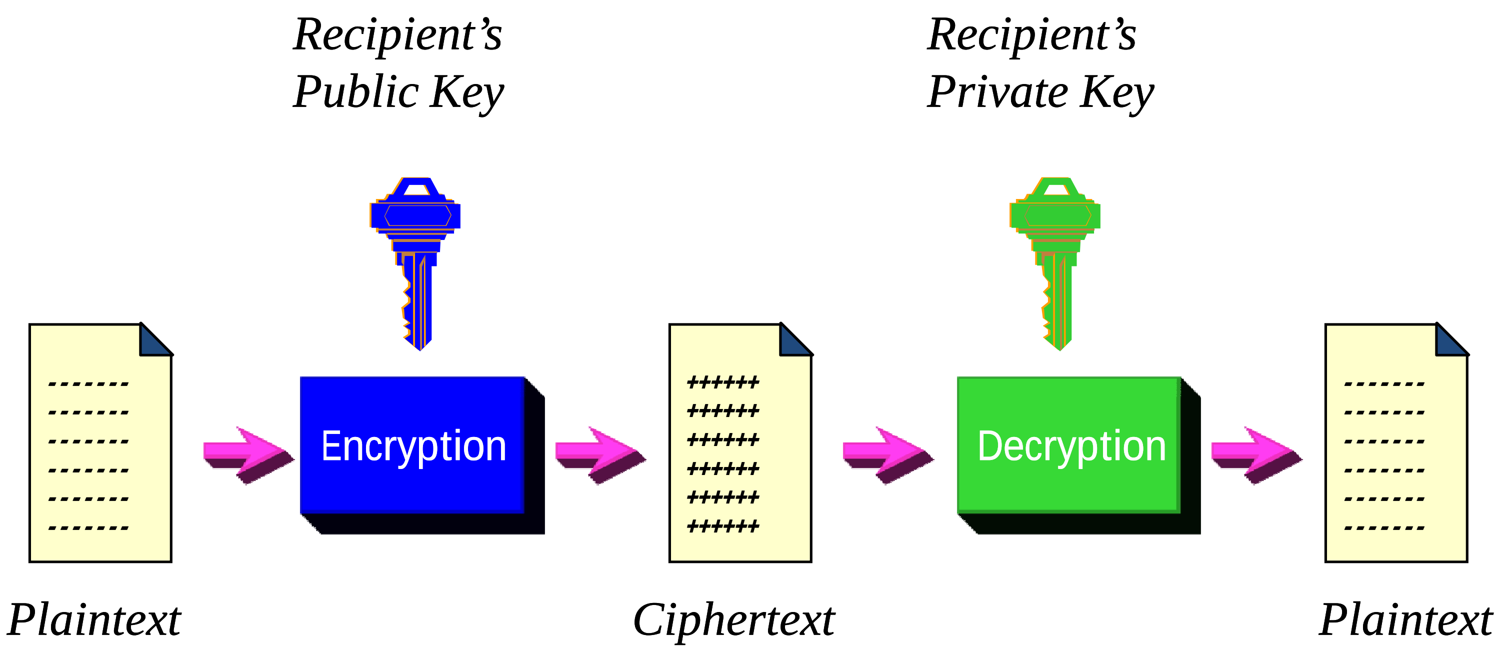
Secret Key Pairs



# of Keys = n * (n – 1)/2

Where n is the # of users

Asymmetric Key Encryption



PKE Algorithm Components

- One or more Prime Numbers
- Large integer factoring
- Modular arithmetic
- Big integer exponentiation
- Example Algorithms
  - Rivest-Shivar-Adelman (RSA)
  - Diffie-Hellman Key Exchange

RSA Public Key Encryption

- Developed by MIT professors Ron Rivest, Adi Shamir and Len Adleman (1977)
- Message blocks treated as a large number less that some number *n*
- Block size 2^k bits ⇨ $2^k < n < 2^{k+1}$
- Relies on:
  - Large prime numbers
  - Large number factoring
  - Modular arithmetic

RSA Key Generation

- Select 2 prime numbers, p and q
- Let $n = p * q$
- Let $\phi(n) = (p – 1)(q – 1)$
- Pick e that is *relatively prime* to $\phi(n)$
- Find d ⇨ $d = e^{-1} \mod \phi(n)$ ⇨ $de = 1 \mod \phi(n)$
- Generated keys:
  - Public: e & n
  - Private: d & n

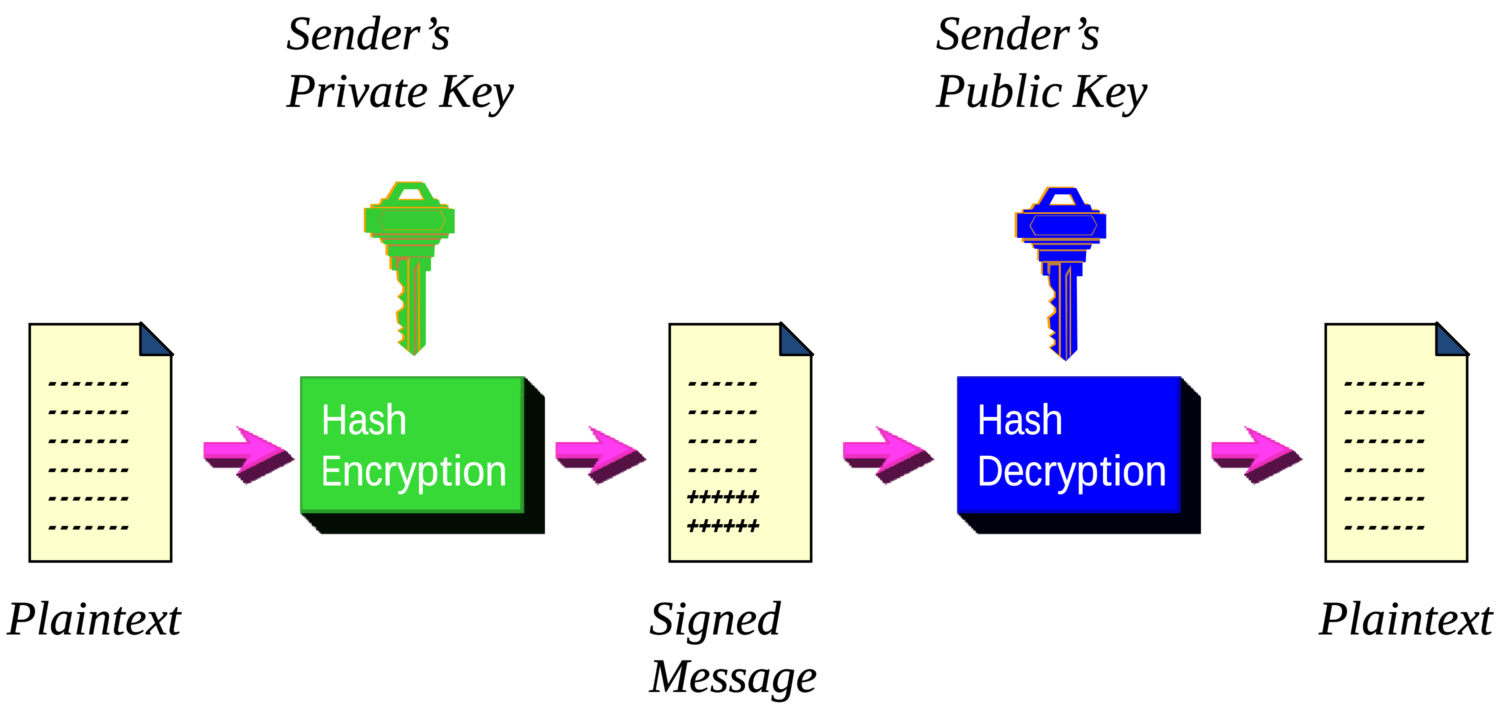
RSA Encryption & Decryption

- Encryption:
  - Break message into M sized blocks < n
  - Cipher $C = M^e \bmod n$
- Decryption:
  - Message $M = C^d \bmod n$

RSA Example

- Key Generation:
  - Let p = 5 and q = 11
  - N = 5 * 11 = 55
  - $\phi(n) = (5 – 1)(11 – 1) = 40$
  - Let e = 3
  - Find d ⇨ 3d = 1 mod 40; d = 27
- Encrypt M = 5 ⇨ C = 5^3 mod 55 = 15
- Decrypt C ⇨ M = 15^{27} mod 55 = 5

Digital Signatures



One-Way Encryption

- Encryption function has no inverse
- Referred to as Hashes or Checksums
- Uses
  - Authentication Systems
  - File Integrity Checkers
  - Message Digests

Hash Functions

- Accept messages of *any* size and generated a small, fixed size output
- One way function
- Easy and fast to calculate
- Collision Resistant

XOR Example

- Break message into fixed length blocks
- XOR first element of all blocks
- Repeat for all elements

G	0100 0111
o	0110 1111
n	0110 1110
o	0110 1111
w	0110 0111
	0101 1110
	5 E

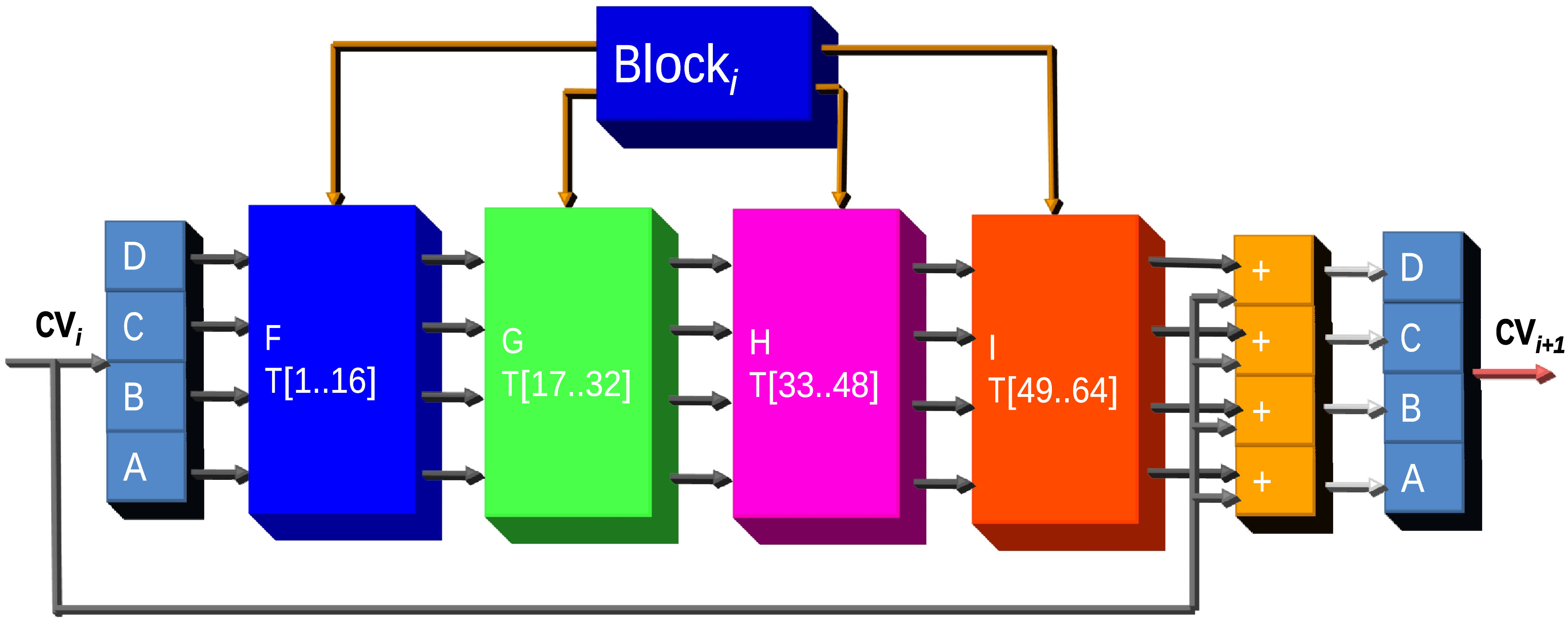
Not very collision resistant!!!

Source: Classical and Contemporary Cryptology
by Richard J. Spillman

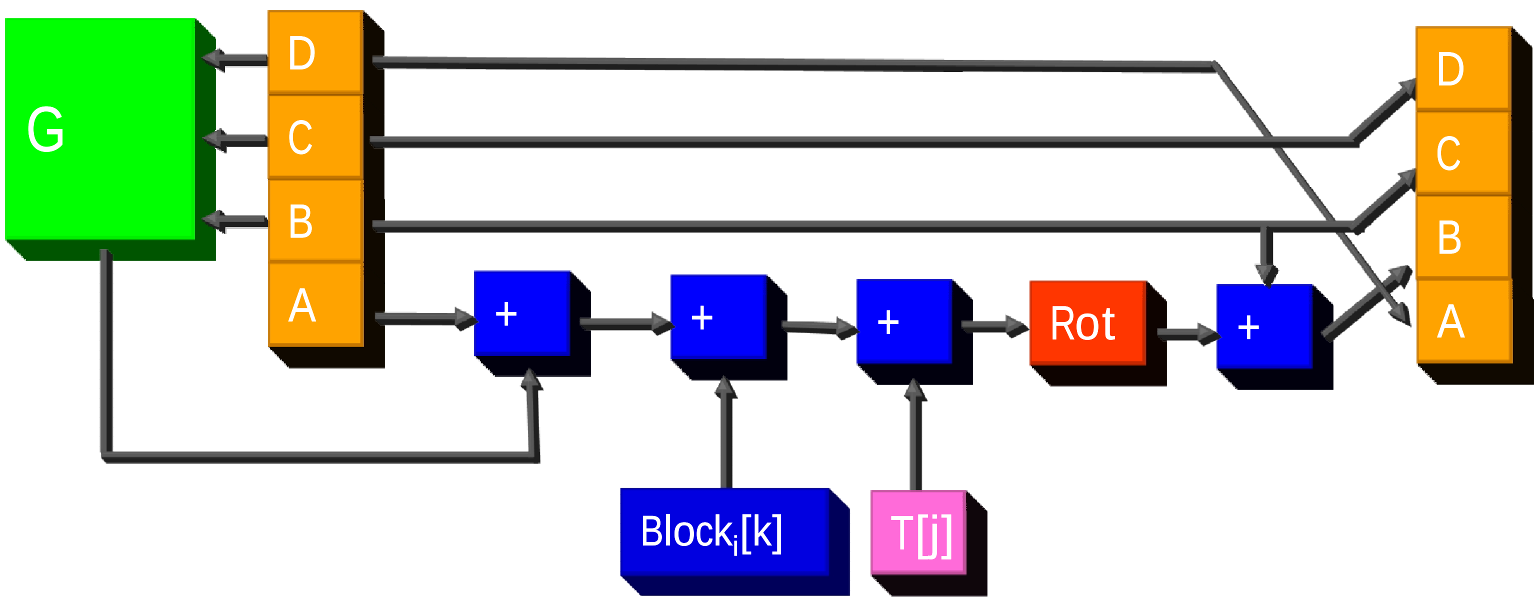
MD5 Hash

- Developed by Ron Rivest
- Generates a 128-bit hash
- Initialization
  - Pad message (1 followed by *n* 0s) such that the message size is 448 mod 512
  - (message size) mod 2^{64} appended to message as 64-bit number
  - 4 32-bit registers used store intermediate and final results
  - 512-bit message block processed in 4 rounds, each consisting of 16 stages

MD5 Rounds



MD5 Stage



Diffie-Hellman Key Exchange

- Bob and Alice together select a prime number, p, and a base, g
- Alice:
  - Selects secret number a
  - Sends Bob g^a mod p
- Bob:
  - Selects secret number b
  - Sends Alice g^b mod p
- Shared secret: k
  - $k = (g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$
  - Used as key in symmetric cryptography algorithm