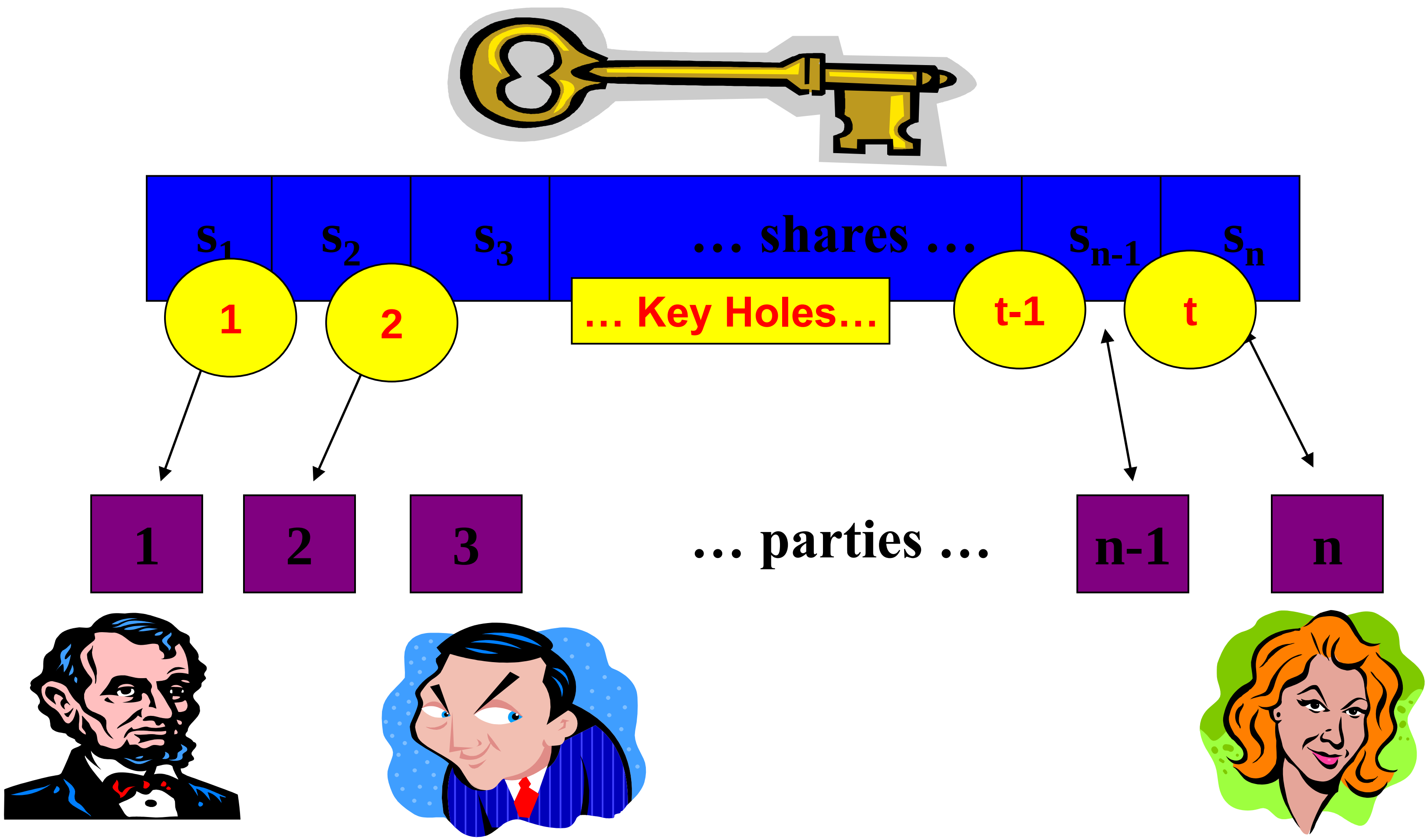
Week 13: Secret Sharing and Threshold Cryptography

Secret Sharing

- **Background**
  - Some secrets are too important to be kept by one person.
  - "*It is easier to trust the many than the few*"
  - Secrecy (trust) and robustness
- **Example:**
  - Purported by Time Magazine in 1992 that the Russian nuclear weapon systems were protected by a two-out-of-three access mechanism – President, Defense Minister and Defense Ministry
- **Secret Sharing**
  - Distribute a secret amongst a group of participants
  - Each participant is allocated a share of the secret
  - Secret can be reconstructed only when the shares are combined together
  - Individual shares are of no use on their own.

Secret Sharing (Schematic)



Secret Sharing

- **Flawed secret sharing**

password → **pa** **ss** **wo** **rd**

Flawed

- **Trivial secret sharing**

  A secret s is distributed as $s = b_1 \oplus b_2 \oplus \ldots \oplus b_{n-1} \oplus b_n$

  1) Choose random numbers $b_1, \ldots, b_{n-1}$

  2) Compute $b_n = b_1 \oplus b_2 \oplus \ldots \oplus b_{n-1} \oplus s$

All n shares should be present to recover the secret s (Not robust)

Wrong Secret Sharing

- **Flawed secret sharing**

password → **pa** **ss** **wo** **rd**   **Flawed**

- **Trivial secret sharing**

  A secret *s* is distributed as $s = b_1 \oplus b_2 \oplus \ldots \oplus b_{n-1} \oplus b_n$

  1) Choose random numbers $b_1, \ldots, b_{n-1}$

  2) Compute $b_n = b_1 \oplus b_2 \oplus \ldots \oplus b_{n-1} \oplus s$

All *n* shares should be present to recover the secret *s* (Not robust)

Threshold Secret Sharing

- Scenario
  - For example, imagine that the Board of Directors of Coca-Cola would like to protect Coke's secret formula. The president of the company should be able to access the formula when needed, but in an emergency any 3 of the 12 board members would be able to unlock the secret formula together.
  - This can be accomplished by a secret sharing scheme with t = 3 and n = 15, where 3 shares are given to the president, and 1 is given to each board member.

- Security Issues
  - Secrecy: resistance against any misbehavior
  - Robustness: reliability against any possible error

SS by Shamir(1/3)

- **(t, n) Secret Sharing**
  - ✓**Secret information *K***
  - ✓***n* share holders ($P_1,\dots,P_n$)**
  - ✓**Using *t-1* degree random polynomial with random coefficient**

(Step 1. Polynomial construction) A dealer selects a secret, *K* (< *p* : prime) as a constant term and *t-1* degree random polynomial with arbitrary coefficients as :

$$F(x) = K + a_1x + a_2x^2 + \dots + a_{k-1}x^{t-1} \bmod p$$

(Step 2. Share distribution) Distributes *F(i) (i=1,…,n)* securely to share holders P_i.

(Step 3. Secret recovery) When *t* shares $\Lambda=(K_1, K_2,\dots,K_t)$ among *n* are given, recover *K* by using the <u>*Lagrange Interpolation*</u>

$$K = \sum_{j\in\Lambda} K_j \lambda_{j,\Lambda} \bmod p, \quad \text{where } \lambda_{j,\Lambda} = \prod_{l\in\Lambda\setminus\{j\}} \frac{l}{l-j}$$

SS by Shamir(2/3)

- ✓**Setup**
  - ✓**(3,5) secret sharing**
  - ✓**K=11, p=17**
  - ✓**Construct a degree 2 random polynomial**

    $F(x) = K + a_1 x + a_2 x^2 \bmod p$
  - ✓**For a random choice** $a_1=8,\ a_2=7$

    $F(x) = 11 + 8x + 7x^2 \bmod 17$
- ✓**GENSHARE**
  - ✓**Share distribution**

$$K_1 = F(1) = 7\times 1^2 + 8\times 1 + 11 \equiv 9 \quad \bmod 17$$
$$K_2 = F(2) = 7\times 2^2 + 8\times 2 + 11 \equiv 4 \quad \bmod 17$$
$$K_3 = F(3) = 7\times 3^2 + 8\times 3 + 11 \equiv 13 \quad \bmod 17$$
$$K_4 = F(4) = 7\times 4^2 + 8\times 4 + 11 \equiv 2 \quad \bmod 17$$
$$K_5 = F(5) = 7\times 5^2 + 8\times 5 + 11 \equiv 5 \quad \bmod 17$$

K_1, K_2, K_3, K_4, K_5 **: shares given to** $(P_1,\ldots,P_5)$

SS by Shamir (3/3)

Using the Lagrange interpolation

For $\Lambda=(K_1, K_2, K_3)$

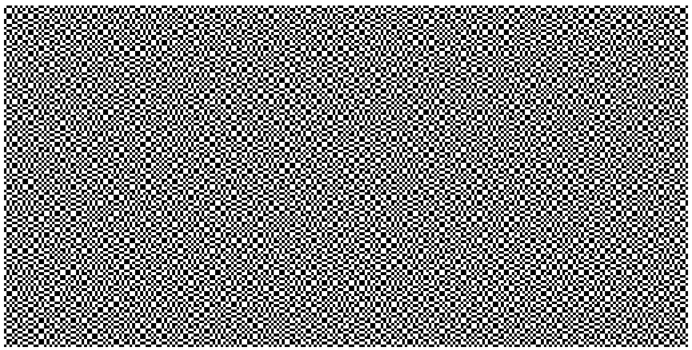
$$K = K_1\left(\frac{2}{2-1}\frac{3}{3-1}\right) + K_2\left(\frac{1}{1-2}\frac{3}{3-2}\right) + K_3\left(\frac{1}{1-3}\frac{2}{2-3}\right)$$

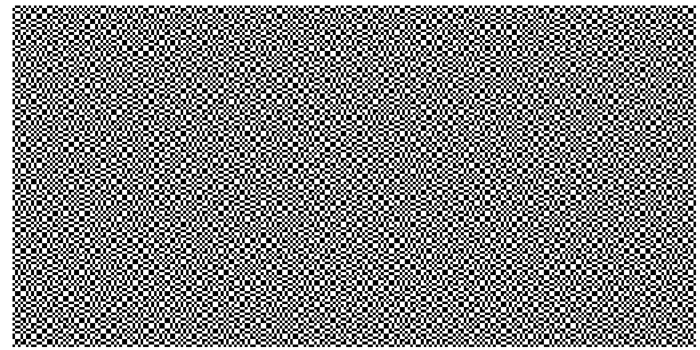
$$= 9\cdot 3 + 4\cdot(-3) + 13\cdot 1 \bmod 17 = 11$$

(Quiz) Using $\Lambda=(K_2, K_4, K_5)$, recover secret, K

(B&W) Visual Cryptography

- What?





  - It is different from the concept of traditional cryptography
  - It depends on perception by the human eyes

Color Visual Cryptography