Internet Security

Common Mistakes in Using Crypto

Mistake #1: Don't know that encryption is needed.

Case Study: U.S. Drones

THE WALL STREET JOURNAL.
U.S. EDITION Thursday, December 17, 2009

Insurgents Hack U.S. Drones

$26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected

Article | Video | Comments (343)

Share

Email | Print | Save

A A

By SIOBHAN GORMAN, YOCHI J. DREAZEN and AUGUST COLE

WASHINGTON -- Militants in Iraq have used $26 off-the-shelf software to intercept live video feeds from U.S. Predator drones, potentially providing them with information they need to evade or monitor U.S. military operations.

Mistake #2: Inventing your own encryption algorithm

Mistake #3: Hard-Coding secret key or storing key with data

Voting machine

DES

Mistake #4: Generate random number incorrectly

```
void main()
{
  int i;
  char key[KEYSIZE];

  printf("%lld\n", (long long) time(NULL));
  srand (time(NULL));        ①

  for (i = 0; i< KEYSIZE; i++){
     key[i] = rand()%256;
     printf("%.2x", (unsigned char)key[i]);
  }
  printf("\n");
}
```

8 ~ 10

```
Plaintext:  255044462d312e350a25d0d4c5d80a34
Ciphertext: d06bf9d0dab8e8ef880660d2af65aa82
IV:         09080706050403020100A2B2C2D2E2F2
```

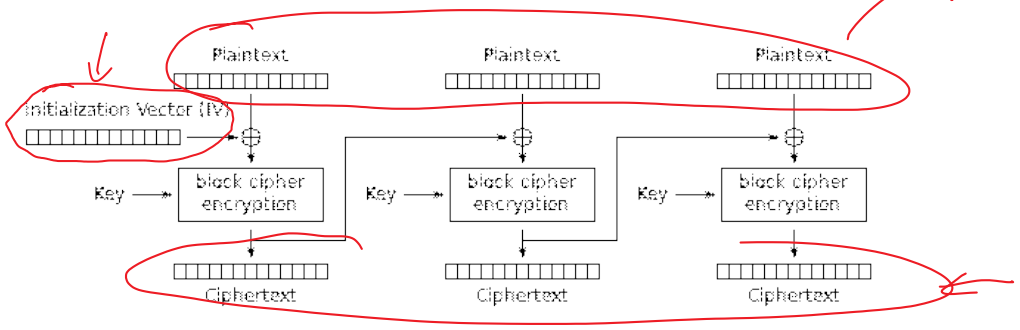
Mistake #5: Use Algorithm Incorrectly

- Still use DES
- Use Wrong Encryption Mode
- Mistakes in the VPN lab
- The IV must be random and unpredictable
- The IV and ciphertext must be authenticated
- Don't encrypt your IVs

Initial Vectors

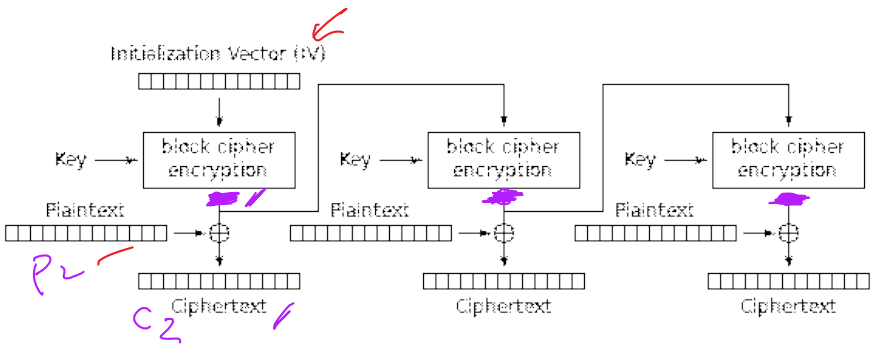
❖ IV cannot repeat

Yes



Cipher Block Chaining (CBC) mode encryption

Known-Plaintext Attack Model:



Output Feedback (OFB) mode encryption

same IV

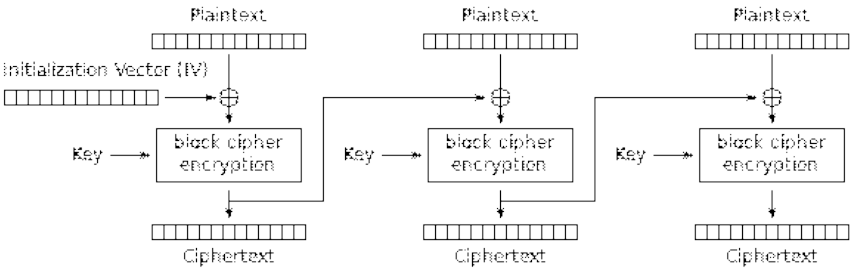
P_1 C_1

P_2 C_2

❖ IV cannot be predictable

Chosen-Plaintext Attack Model:

P_1 C_1 ? Yes No



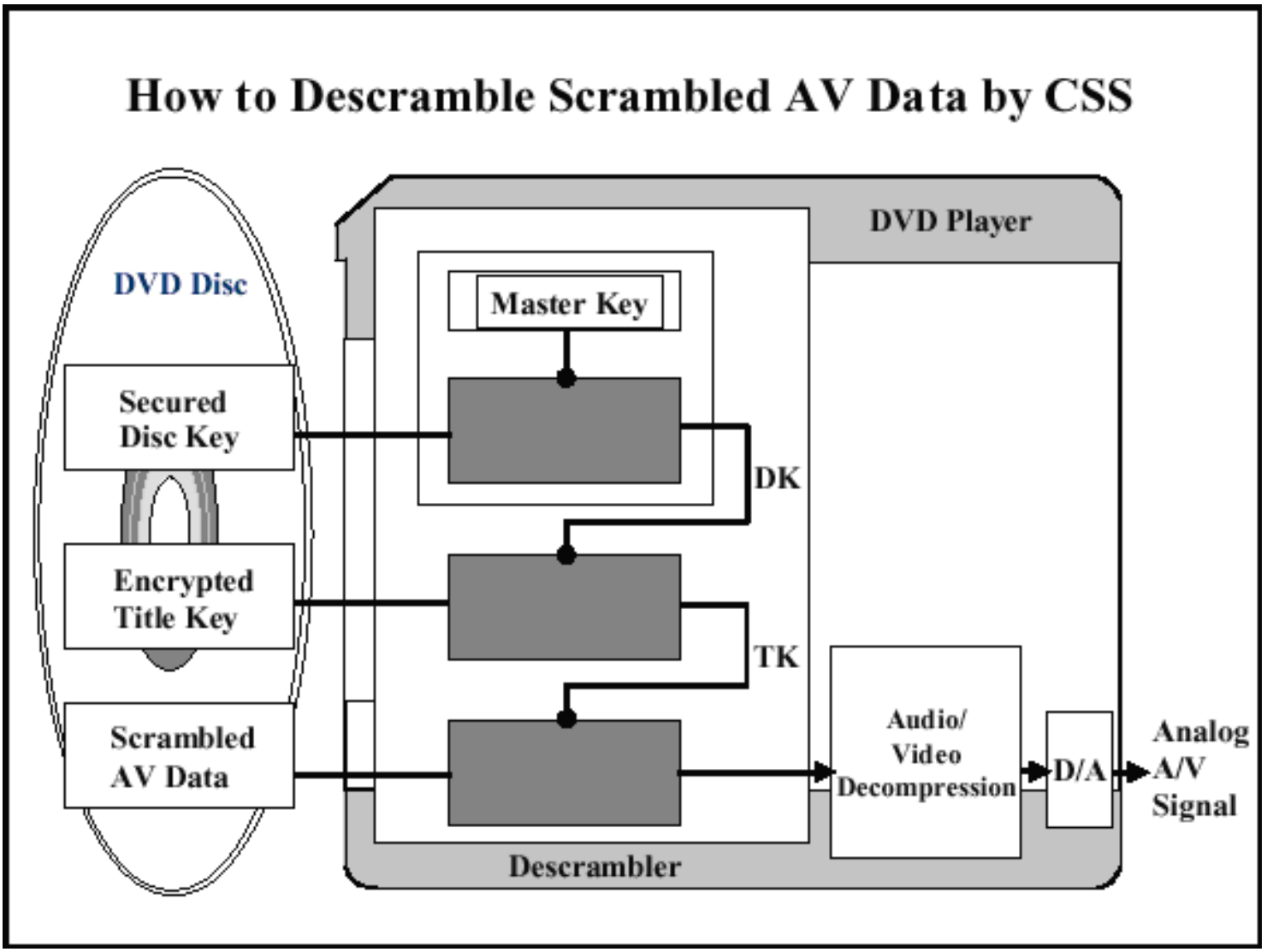
Cipher Block Chaining (CBC) mode encryption

Mistake #6: Keeping keys in memory for unnecessarily long

Mistake #7: Key Management

FBI-vs-Apple: Case Study

Case Study: DVD Protection



Case Study: Smartcards