Initialization Vectors

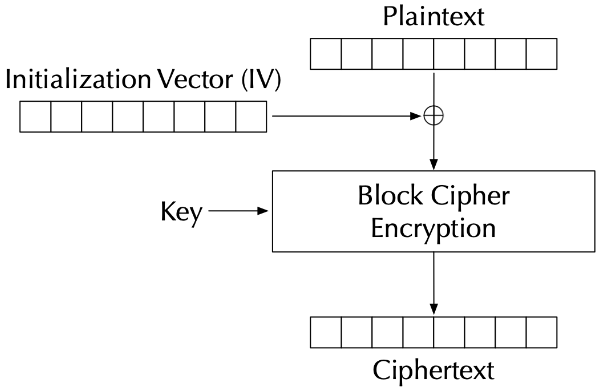
- IV: *what is it?* and *why do we need it?*
- Requirements for IVs
- Common Mistakes & Attacking Poorly Chosen IVs

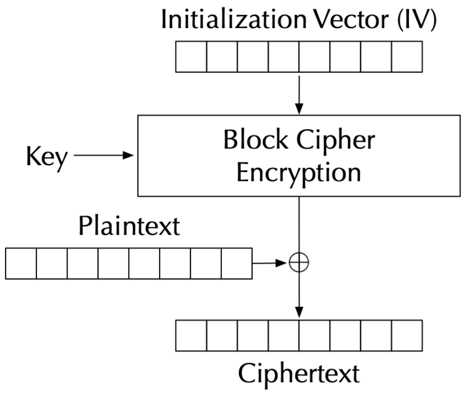
Initialization Vectors and Common Mistakes

- Initialization Vectors have the following requirements:
  - IV is supposed to be stored or transmitted in plaintext
  - IV should not be reused -> uniqueness
  - IV should not be predictable -> pseudorandom

- Some modes w/ IVs:

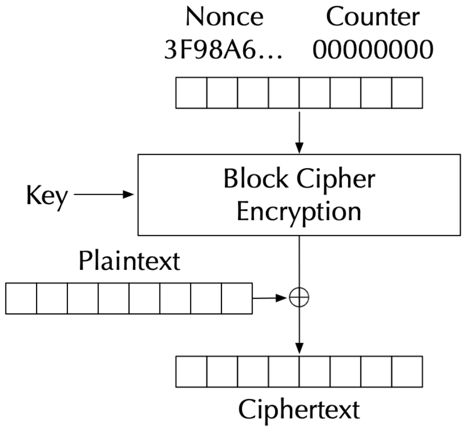
CBC

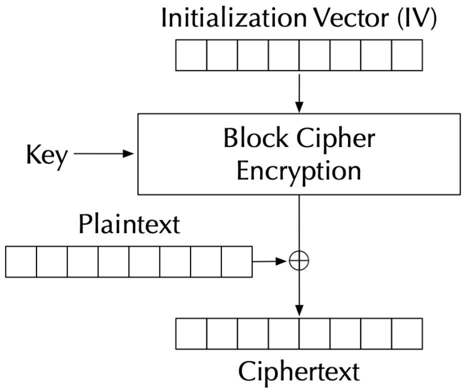




CFB

CTR





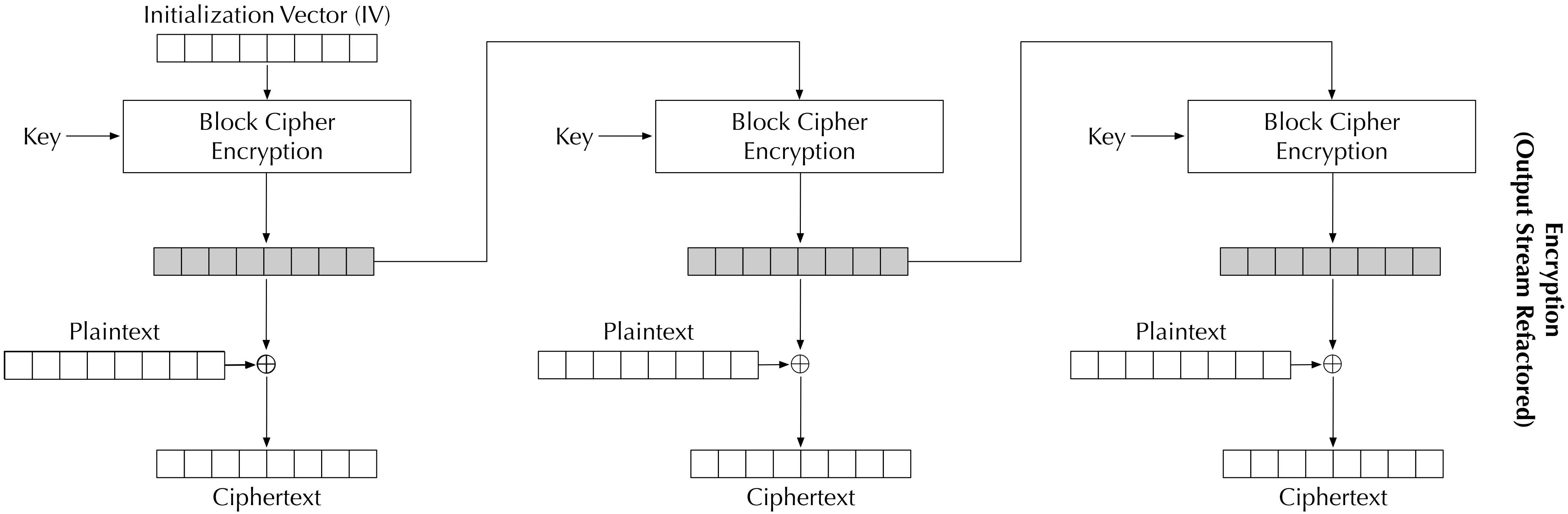
OFB

IV should not be **reused**...

Scenario:

- Suppose attacker knows some info about plaintexts ("known-plaintext attack")
- Plaintexts encrypted using AES-128-OFB **and the same IV is repeatedly used**...

Attacker Goal: Decrypt other plaintexts

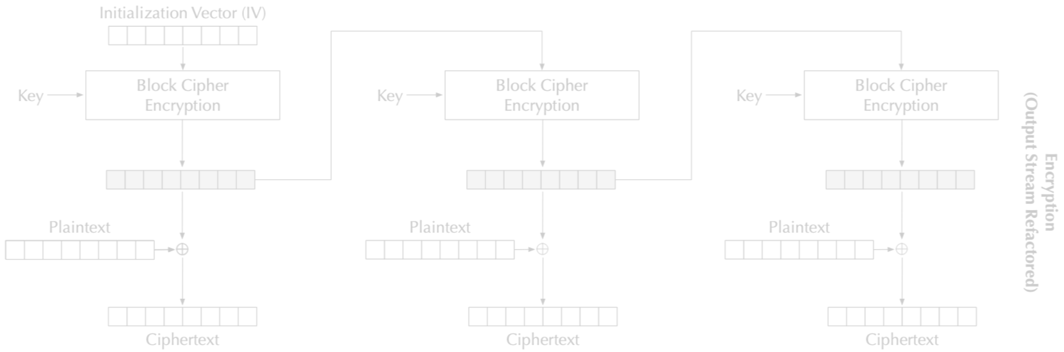


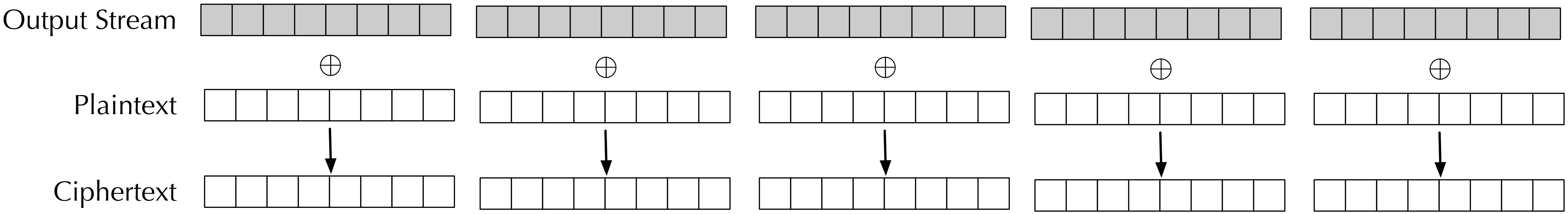
IV should not be **reused**...

Scenario:

- Suppose attacker knows some info about plaintexts ("known-plaintext attack")
- Plaintexts encrypted using AES-128-OFB **and the same IV is repeatedly used**...

Attacker Goal: Decrypt other plaintexts





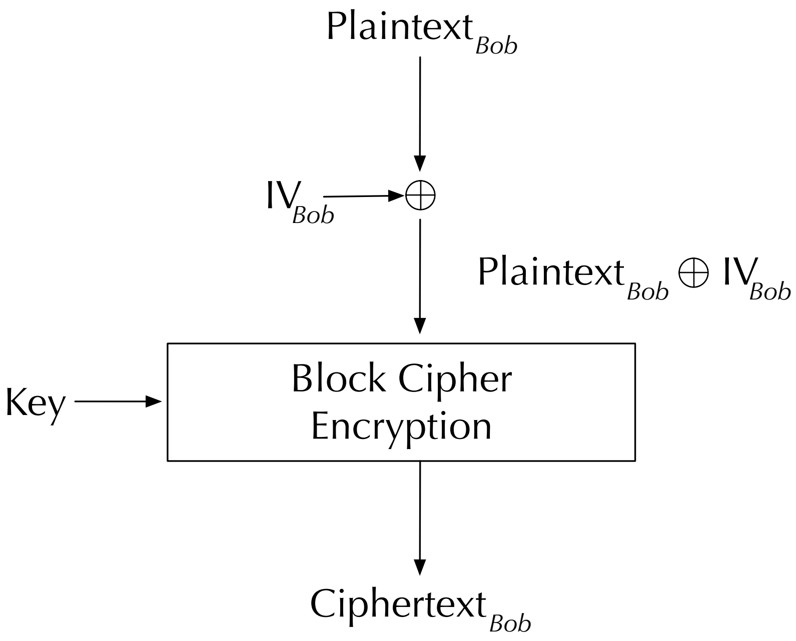
Encryption
(Simplified)

IV should not be **predictable**…

Scenario:

- Suppose attacker can get victim to encrypt some chosen plaintexts ("chosen-plaintext attack")
- Plaintext messages are highly structured / there are few options (e.g., "Yes"/"No", name of presidential candidate)
- Plaintexts encrypted using AES-128-CBC **and the IVs are predictable**…

Attacker Goal: Learn contents of other plaintexts

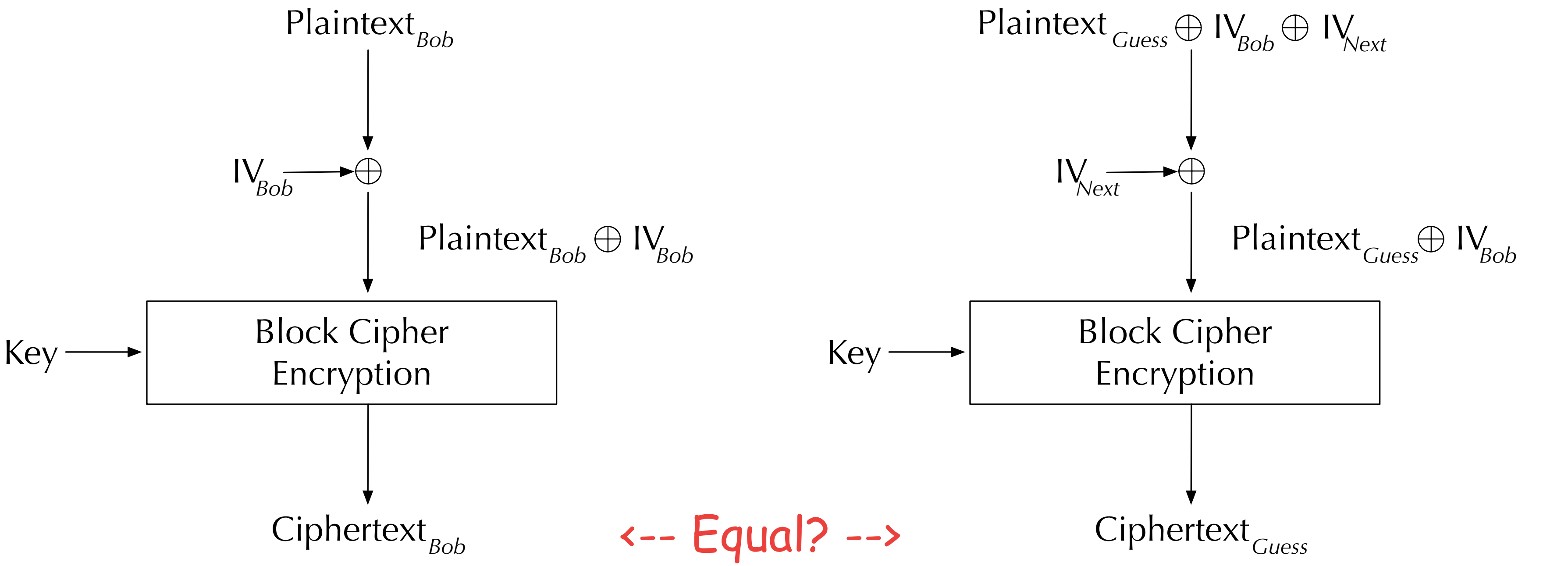


IV should not be **predictable**...

Scenario:

- Suppose attacker can get victim to encrypt some chosen plaintexts ("chosen-plaintext attack")
- Plaintext messages are highly structured / there are few options (e.g., "Yes"/"No", name of presidential candidate)
- Plaintexts encrypted using AES-128-CBC and the IVs are predictable...

Attacker Goal: Learn contents of other plaintexts


Plaintext_{Bob}
IV_{Bob}
$\text{Plaintext}_{Bob} \oplus IV_{Bob}$
Key
Block Cipher Encryption
Ciphertext_{Bob}
<-- Equal? -->
$\text{Plaintext}_{Guess} \oplus IV_{Bob} \oplus IV_{Next}$
IV_{Next}
$\text{Plaintext}_{Guess} \oplus IV_{Bob}$
Key
Block Cipher Encryption
$\text{Ciphertext}_{Guess}$