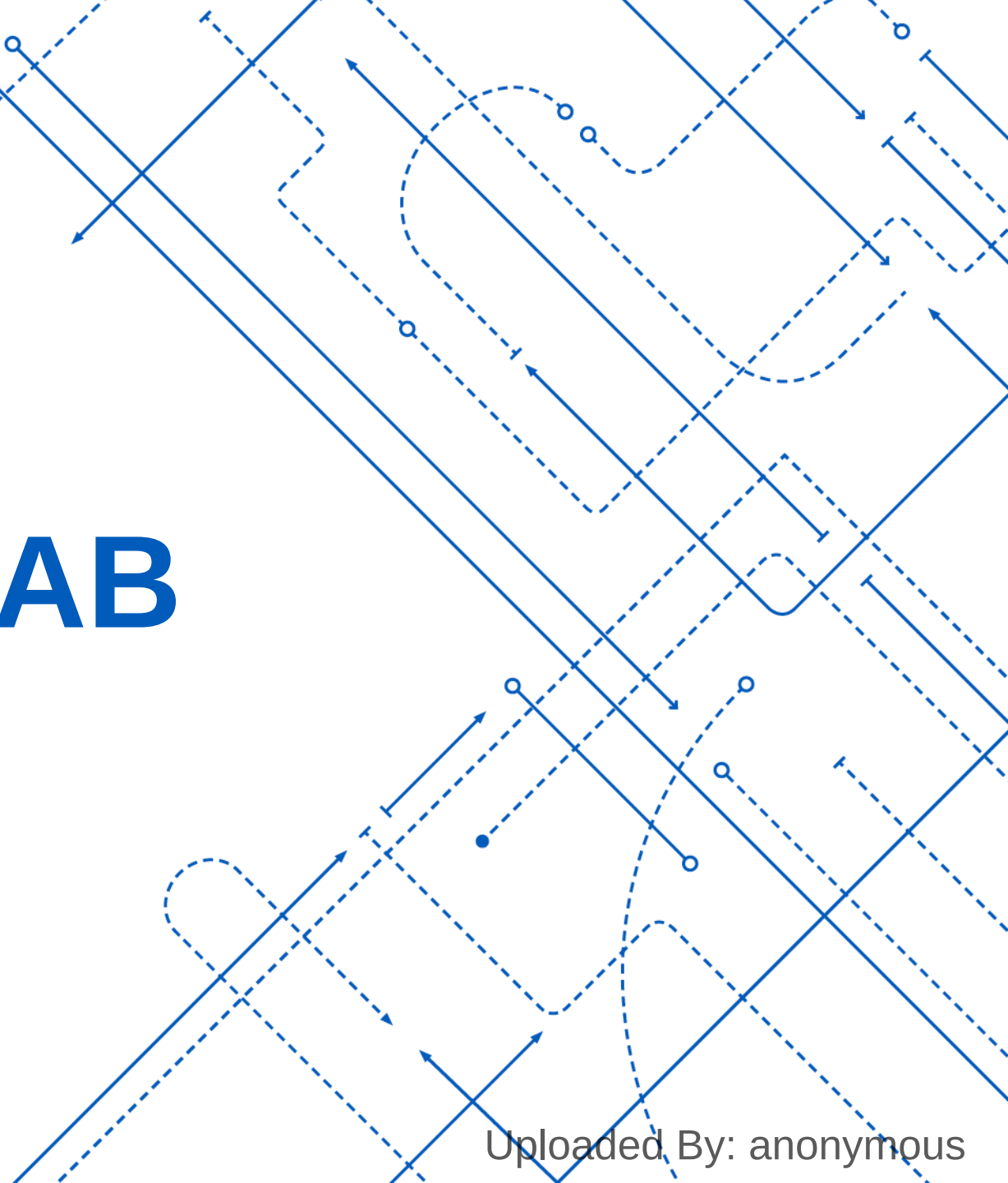
EXP #2

SECRET-KEY ENCRYPTION LAB

SLIDES BY: MOHAMAD BALAWI



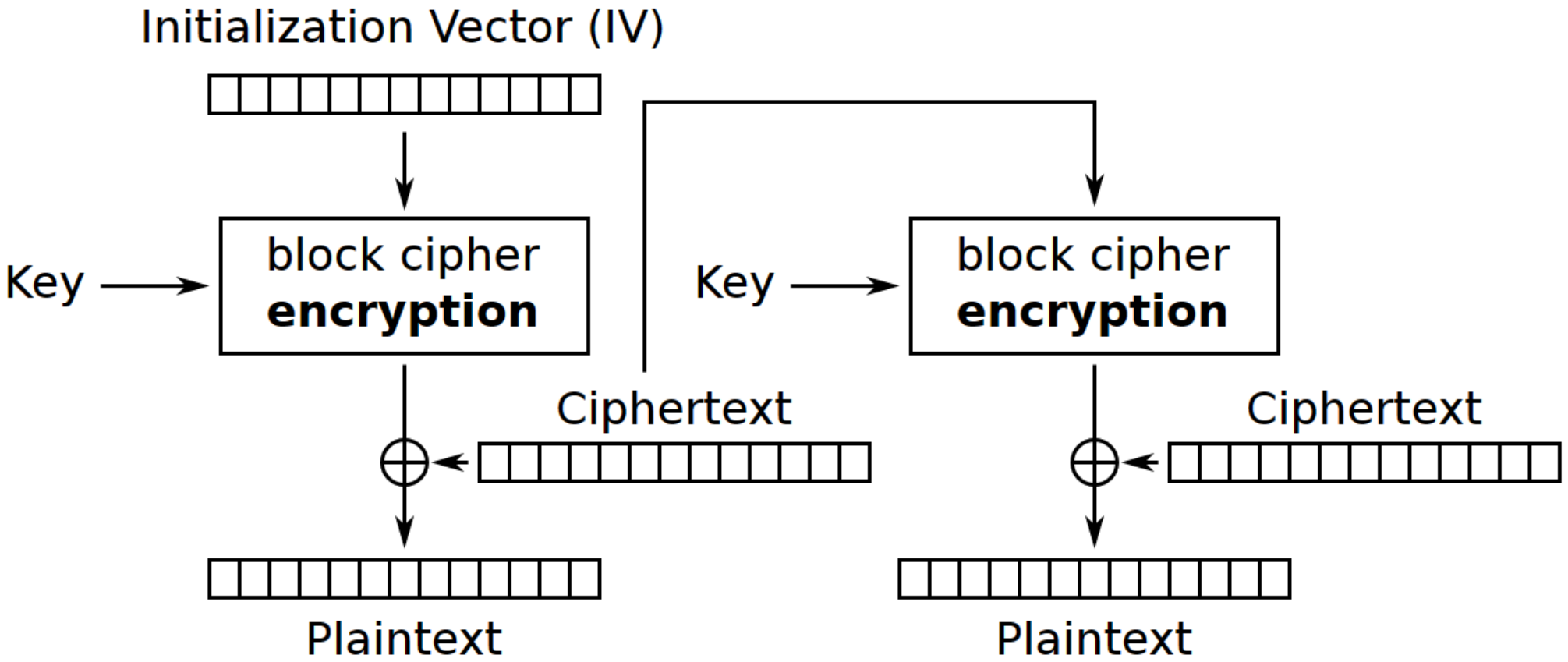
جامعة بيرزيت BIRZEIT UNIVERSITY

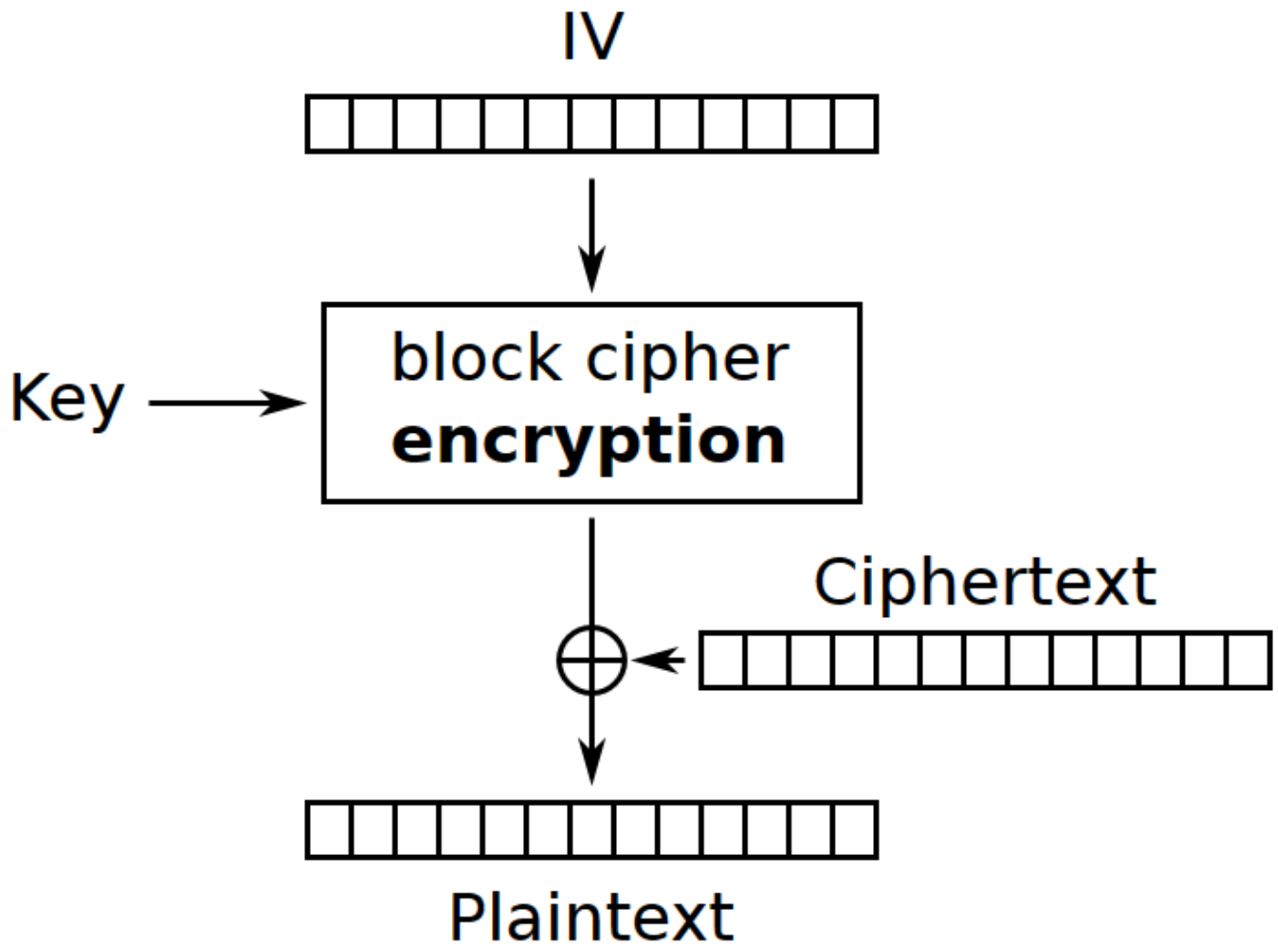
Task 6.2. Common Mistake: Use the Same IV

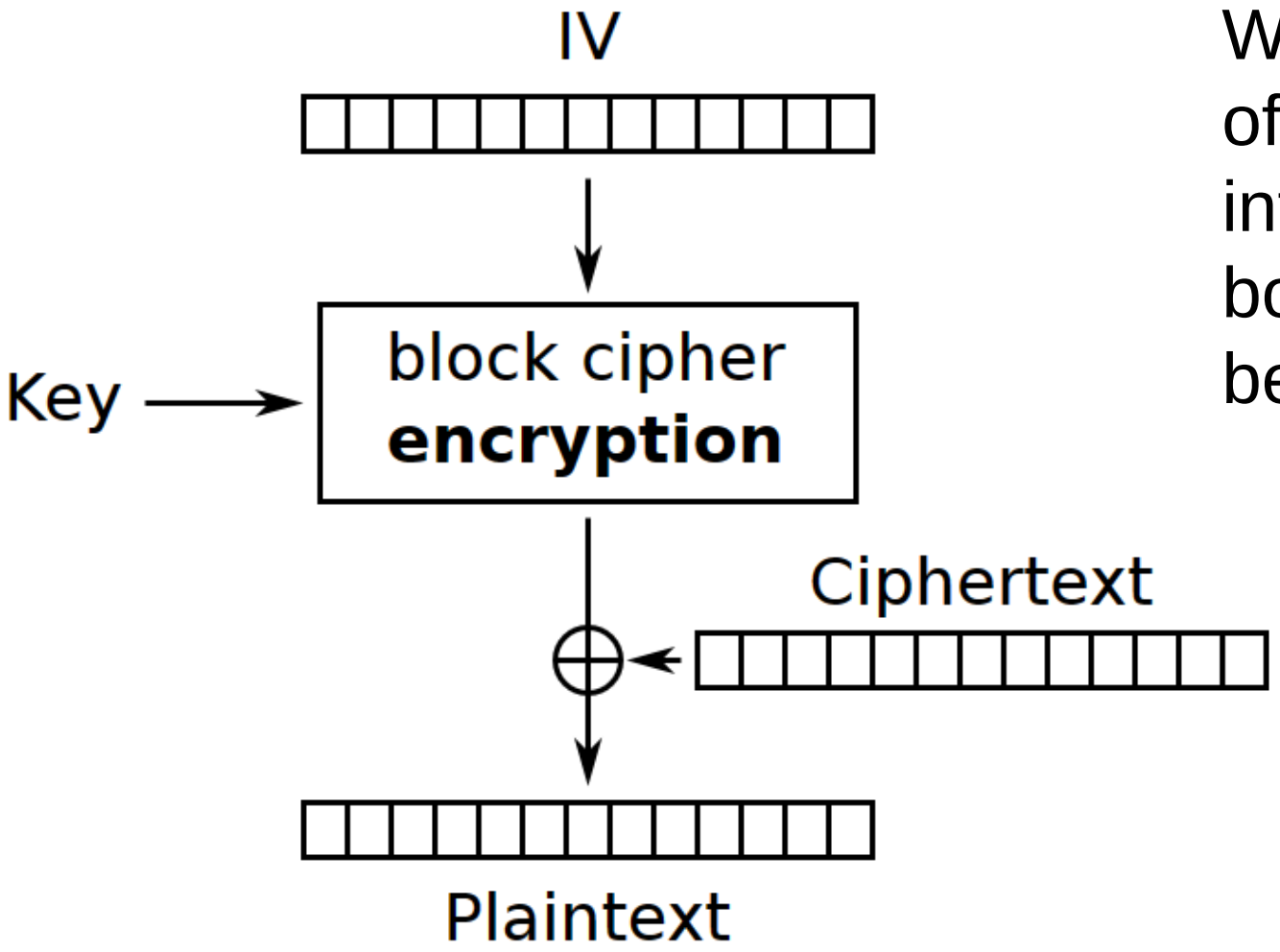
```
Plaintext  (P1): This is a known message!
Ciphertext (C1): a469b1c502c1cab966965e50425438e1bb1b5f9037a4c159

Plaintext  (P2): (unknown to you)
Ciphertext (C2): bf73bcd3509299d566c35b5d450337e1bb175f903fafc159
```

Vulnerable to ***known-plaintext attack.***

Cipher Feedback (CFB) mode decryption



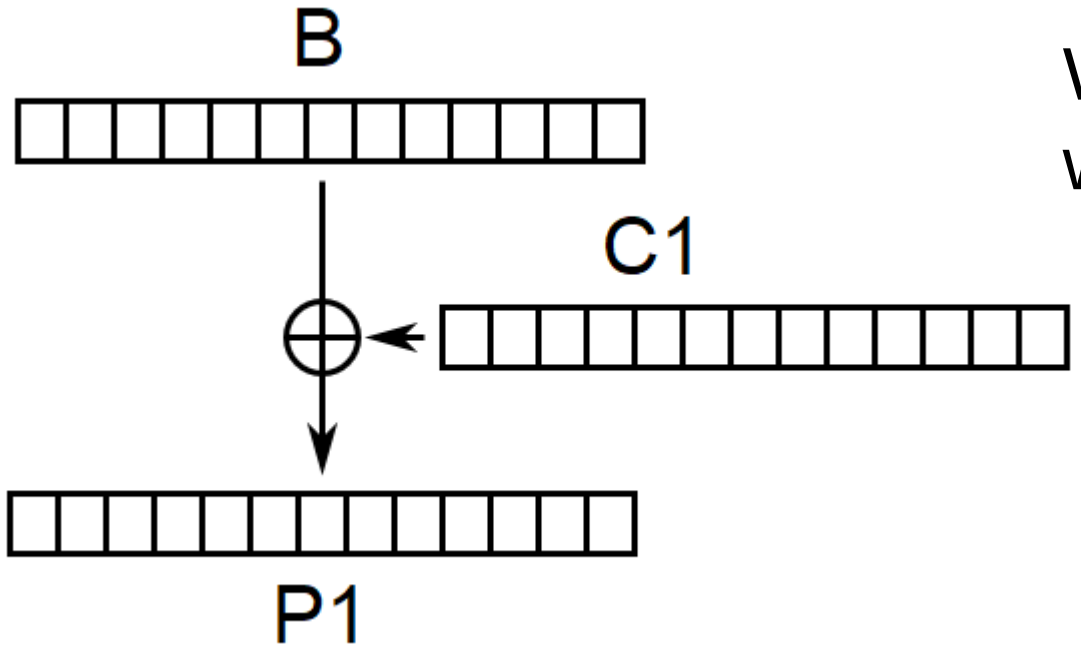




We can abstract the output of “block cipher encryption” into **B** since we know that both IV and Key will always be the same.

The equation for decrypting $\boldsymbol{P_1}$ is:

$$P_1 = C_1 \oplus B$$



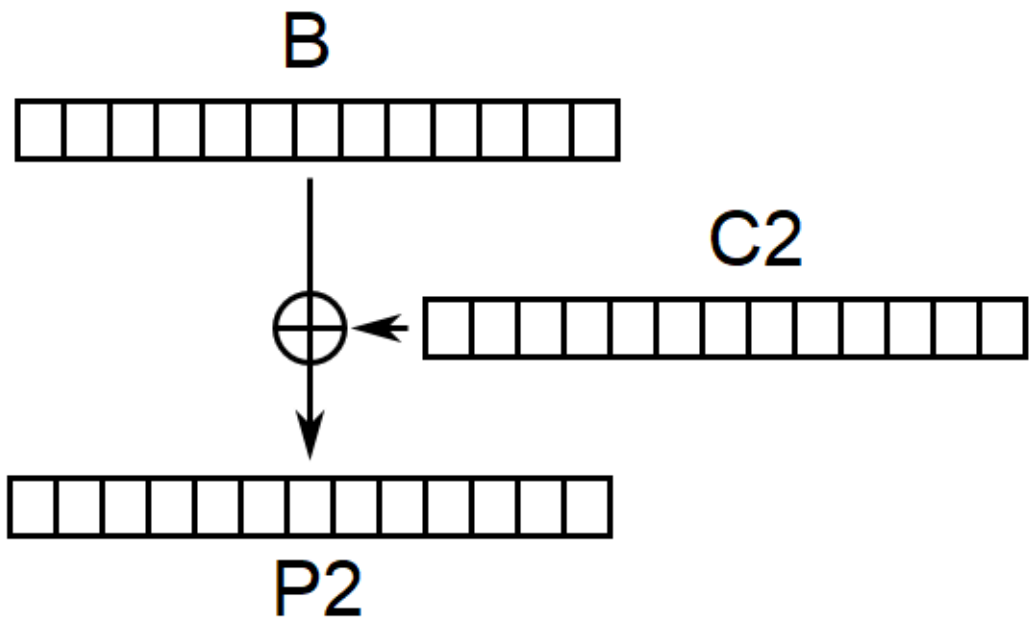
We know the value of $\boldsymbol{P_1}$ and $\boldsymbol{C_1}$ so we can calculate the value of $\boldsymbol{B}$.

$$B = C_1 \oplus P_1$$

The equation for decrypting $\boldsymbol{P_2}$ is:

$$P_2 = C_2 \oplus B$$

We know the value of $\boldsymbol{C_2}$ and $\boldsymbol{B}$ so we can calculate the value of $\boldsymbol{P_2}$

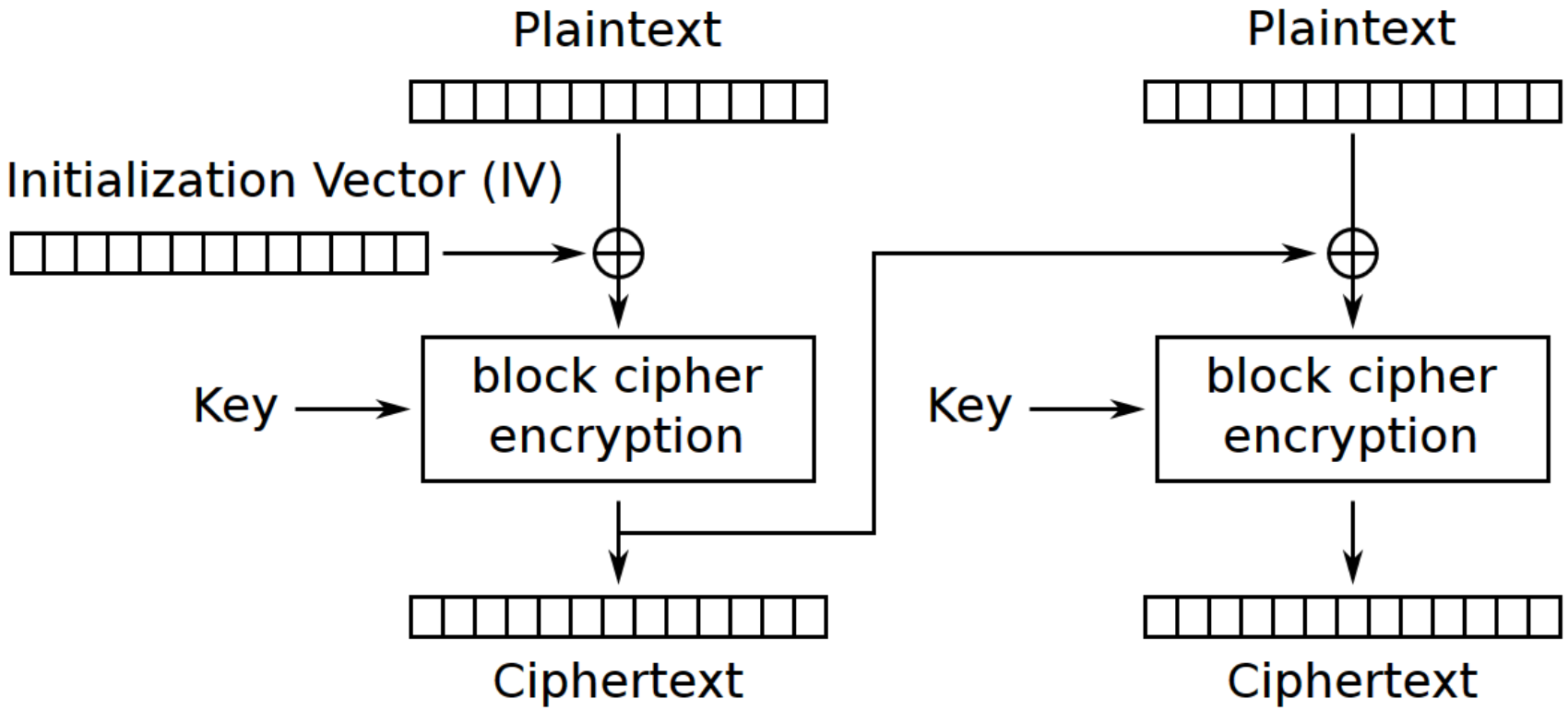


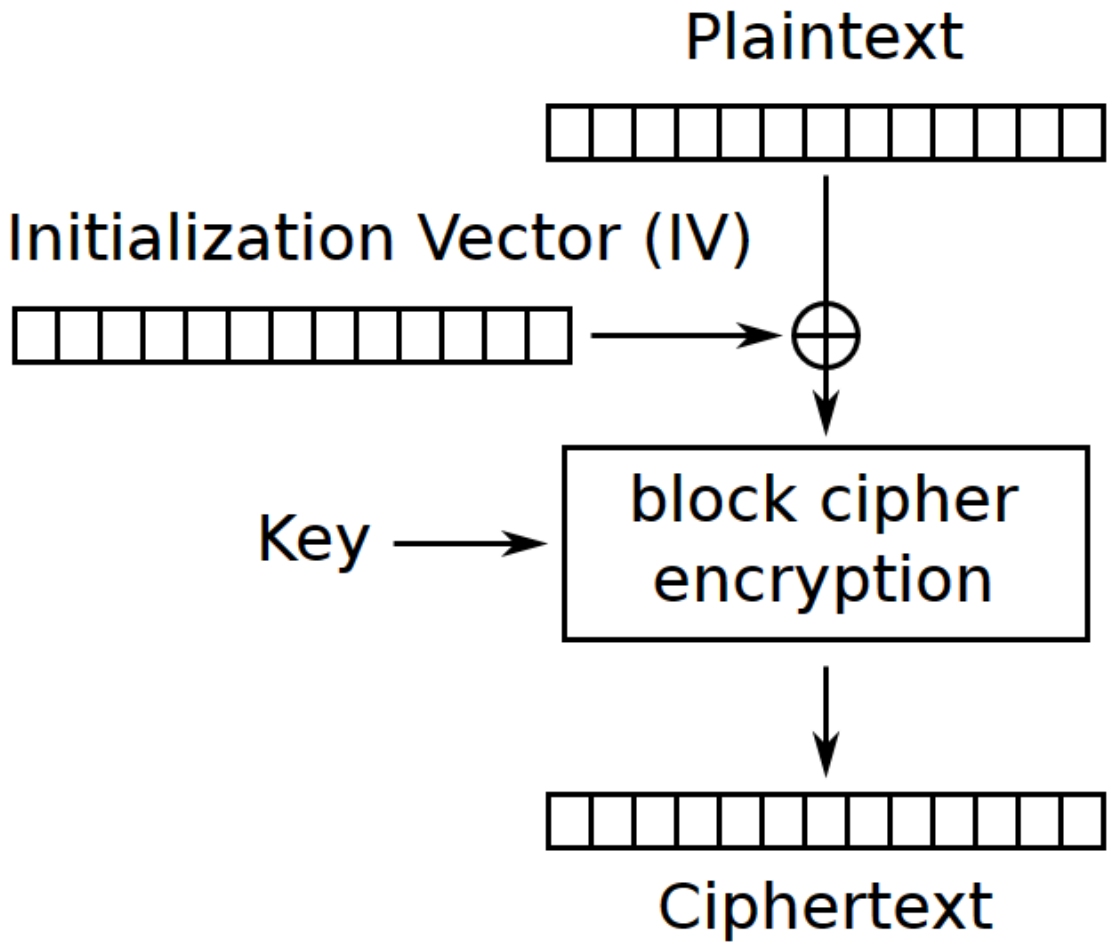
Task 6.3. Common Mistake: Use a Predictable IV

```
$ nc 10.9.0.80 3000
Bob's secret message is either "Yes" or "No", without quotations.
Bob's ciphertex: 54601f27c6605da997865f62765117ce
The IV used    : d27d724f59a84d9b61c0f2883efa7bbc

Next IV        : d34c739f59a84d9b61c0f2883efa7bbc

Your plaintext : 11223344aabbccdd
Your ciphertext: 05291d3169b2921f08fe34449ddc3611

Next IV        : cd9f1ee659a84d9b61c0f2883efa7bbc
Your plaintext : <your input>
```

Vulnerable to ***chosen-plaintext attack.***

Cipher Block Chaining (CBC) mode encryption





Bob's turn

List of known variables:

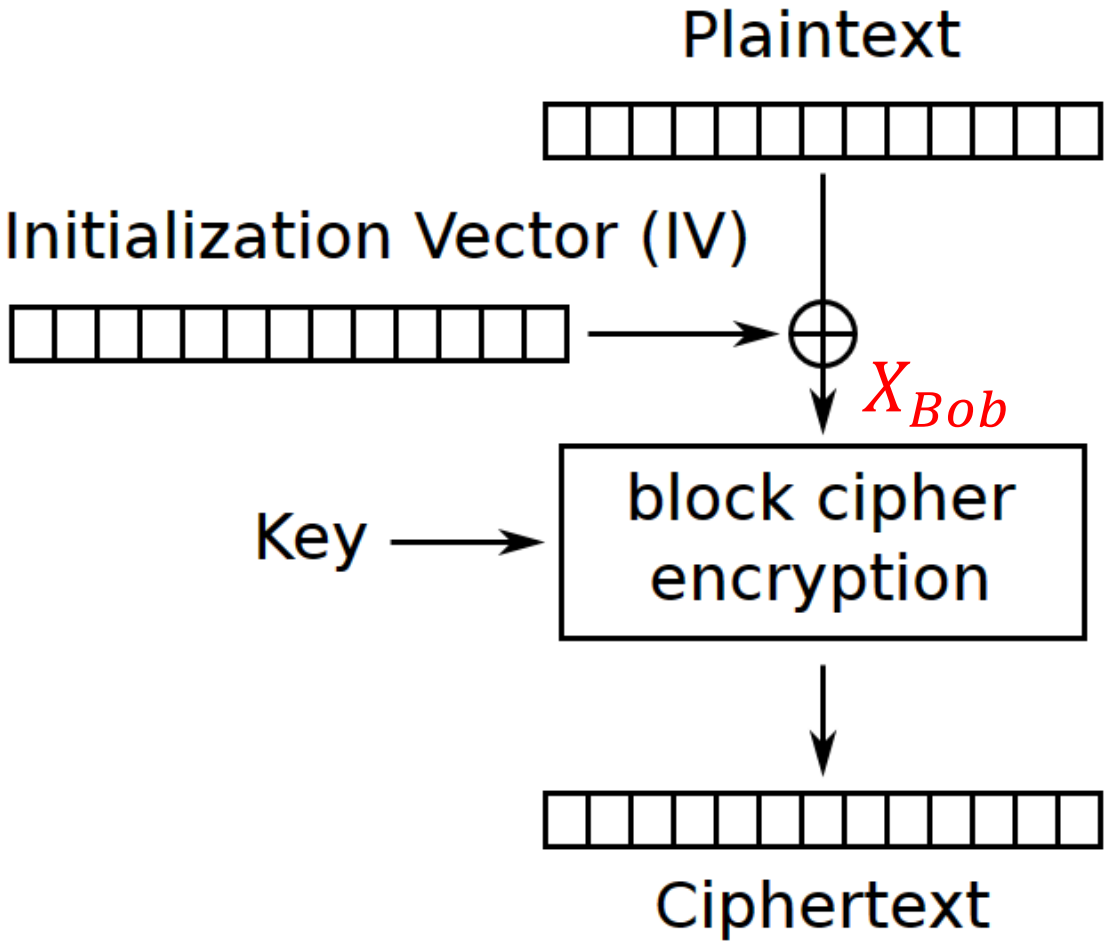
P_{Bob} = "Yes" or "No"

Assume that P_{Bob} = "Yes"

C_{Bob}

IV_{Bob}

IV_{You}



$$X_{Bob} = P_{Bob} \oplus IV_{Bob}$$

Your turn

List of known variables:

$$P_{You} = P_{Bob} \oplus IV_{Bob} \oplus IV_{You}$$

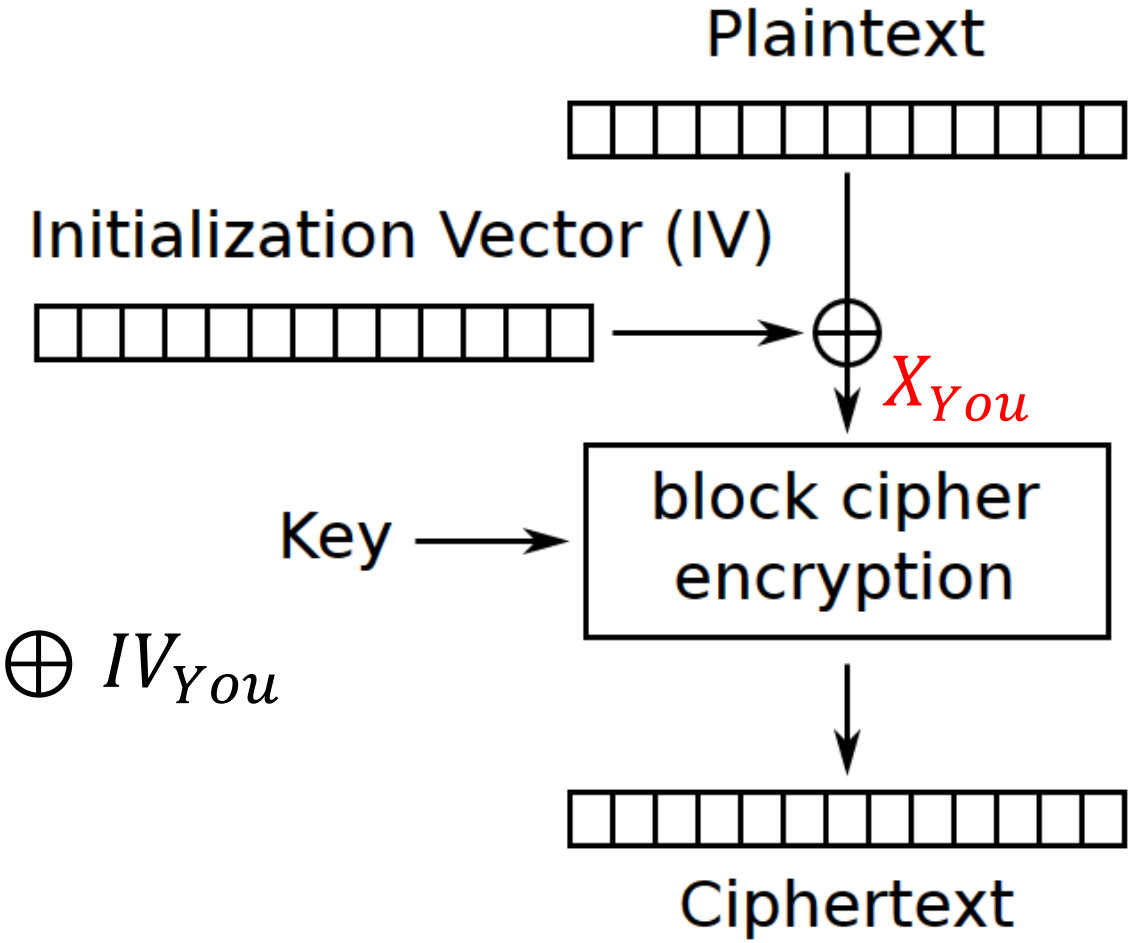
$$X_{You} = P_{You} \oplus IV_{You}$$

$$X_{You} = (P_{Bob} \oplus IV_{Bob} \oplus IV_{You}) \oplus IV_{You}$$

$$X_{You} = P_{Bob} \oplus IV_{Bob}$$

$$X_{You} = X_{Bob}$$

You reproduced Bob's turn.



Note that:

$$X_{You} = X_{Bob}$$

Which means that you have reproduced Bob's turn, so if your ciphertext is the same as Bob's then we know the plaintext is "Yes", else the plaintext is "No"