

```

1 public AESCipher{
2     Cipher cipher;
3     SecretKey key;
4     ...
5     public byte[] encrypt(byte[] data, byte[] data2){
6         //The state-of-the-arts API recommendation solutions make wrong choice here
7         cipher.update(data);
8         //while the correct one should be
9         // cipher.updateAAD(data)
10        return cipher.doFinal(data2);
11    }
12    public Cipher init(){
13        cipher = Cipher.getInstance("AES/GCM/NoPadding");
14        //A "GCM" mode suggests an infrequent API updateAAD may be used later
15        cipher.init(Cipher.ENCRYPT_MODE,key)
16    }
17 }

```

Figure 1: A wrong API choice. Inexperienced developers and state-of-the-arts API recommendation systems cannot figure out the correct API choice (Line 9) but choose a wrong one (Line 7).

The reason for this wrong recommendation is caused by inability to distinguish the code context in Figure 1 and Figure 2.

```

1 public AESCipher{
2     Cipher cipher;
3     SecretKey key;
4     ...
5     public byte[] encrypt(byte[] data, byte[] data2){
6         //A common scenario Cipher.update should be used
7         cipher.update(data);
8         return cipher.doFinal(data2);
9     }
10    public Cipher init(){
11        cipher = Cipher.getInstance("AES/CBC/NoPadding"); //CBC mode
12        //When the mode is not "GCM", Cipher.update is the correct choice
13        cipher.init(Cipher.ENCRYPT_MODE,key)
14    }
15 }

```

Figure 2: A similar code snippet where Line 7 can be used. State-of-the-arts cannot distinguish situations in Figure 1 and Figure 2.