bcgit / **bc-java** Public mirror

mirrored from https://www.bouncycastle.org/repositories/bc-java

Code | Issues 299 | Pull requests 41 | Discussions | Actions | Projects

Commit 701686c

dghgit committed on Dec 17, 2025

```
fixed one off error in G3413CTRBlockCipher
```

main · r1rv84

1 parent 1b6a3dc commit 701686c

2 files changed +2 -4

Top

Filter files…

- core/src
  - main/java/org/bouncycastle/crypto/modes
    - G3413CTRBlockCipher.java
  - test/java/org/bouncycastle/crypto/test
    - GOST3412Test.java

Search within code

...astle/crypto/modes/G3413CTRBlockCipher.java

```
@@ -73,7 +73,6 @@ public void init(
73  73            CipherParameters params)
74  74            throws IllegalArgumentException
75  75        {
76      -
77  76            if (params instanceof ParametersWithIV)
78  77            {
```

```
79  78              ParametersWithIV ivParam = (ParametersWithIV)params;
    @@ -92,7 +91,7 @@ public void init(
92  91              {
93  92                  CTR[i] = 0;
94  93              }
95      -
    94  +
96  95              // if null it's an IV changed only.
97  96              if (ivParam.getParameters() != null)
98  97              {
    @@ -198,7 +197,6 @@ private void generateCTR()
198 197              {
199 198                  throw new IllegalStateException("attempt to process too many
                    blocks");
200 199              }
201     -            CTR[start]++;
202 200          }
203 201      }
204 202
```

.../bouncycastle/crypto/test/GOST3412Test.java

```
    @@ -87,7 +87,7 @@ public String getName()
87  87      public void performTest()
88  88          throws Exception
89  89      {
90      -        //super.performTest();
    90  +        super.performTest();
91  91
92  92          ctrTest();
93  93  //        cfbTest();
```

Comments 0