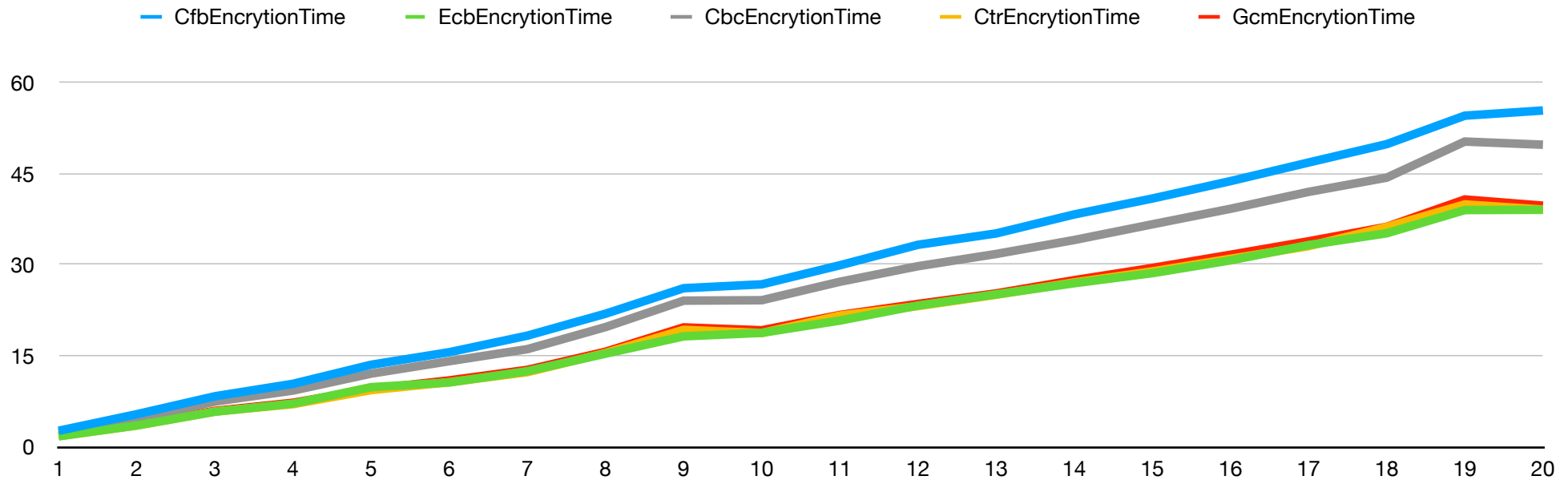


Encryption: The encryption time data is based from various algorithms (AES_CFB, AEC_ECB, AES_CBC, AES_CTR, AES_GCM) across multiple sizes (1 MB to 20 MB) and time consuming are in millisecond.

| | CfbEncryptionTime | EcbEncryptionTime | CbcEncryptionTime | CtrEncryptionTime | GcmEncryptionTime |
|-------|-------------------------|-------------------------|-------------------------|-------------------------|-------------------------|
| 1 | 2.59644985198974609375 | 1.68335437774658203125 | 2.23984718322753906250 | 1.70011520385742187500 | 1.76794528961181640625 |
| 2 | 5.32851219177246093750 | 3.46848964691162109375 | 4.51042652130126953125 | 3.47309112548828125000 | 3.59017848968505859375 |
| 3 | 8.28909873962402343750 | 5.73647022247314453125 | 7.41415023803710937500 | 5.76910972595214843750 | 5.87737560272216796875 |
| 4 | 10.34681797027587890625 | 7.08348751068115234375 | 9.23264026641845703125 | 6.98757171630859375000 | 7.21683502197265625000 |
| 5 | 13.49115371704101562500 | 9.79120731353759765625 | 12.03017234802246093750 | 9.30345058441162109375 | 9.47308540344238281250 |
| 6 | 15.56129455566406250000 | 10.56671142578125000000 | 14.07911777496337890625 | 10.61096191406250000000 | 10.91012954711914062500 |
| 7 | 18.29538345336914062500 | 12.43185997009277343750 | 16.06807708740234375000 | 12.26565837860107421875 | 12.65010833740234375000 |
| 8 | 21.91264629364013671875 | 15.32068252563476562500 | 19.70784664154052734375 | 15.42739868164062500000 | 15.64078330993652343750 |
| 9 | 26.12421512603759765625 | 18.18025112152099609375 | 24.07262325286865234375 | 19.25122737884521484375 | 19.65711116790771484375 |
| 10 | 26.76384449005126953125 | 18.75495910644531250000 | 24.14391040802001953125 | 18.72518062591552734375 | 19.18513774871826171875 |
| 11 | 29.91185188293457031250 | 20.78537940979003906250 | 27.18994617462158203125 | 21.60730361938476562500 | 21.70748710632324218750 |
| 12 | 33.29243659973144531250 | 23.26703071594238281250 | 29.75664138793945312500 | 23.17342758178710937500 | 23.53408336639404296875 |
| 13 | 35.16550064086914062500 | 25.11305809020996093750 | 31.77394866943359375000 | 25.04327297210693359375 | 25.26462078094482421875 |
| 14 | 38.30163478851318359375 | 26.94876194000244140625 | 34.08200740814208984375 | 27.07562446594238281250 | 27.45249271392822265625 |
| 15 | 40.92888832092285156250 | 28.60939502716064453125 | 36.67171001434326171875 | 28.89816761016845703125 | 29.47051525115966796875 |
| 16 | 43.79997253417968750000 | 30.72249889373779296875 | 39.23463821411132812500 | 30.98459243774414062500 | 31.64737224578857421875 |
| 17 | 46.87194824218750000000 | 33.25071334838867187500 | 42.02518463134765625000 | 33.06734561920166015625 | 33.87041091918945312500 |
| 18 | 49.90401268005371093750 | 35.19020080566406250000 | 44.37210559844970703125 | 36.22136116027832031250 | 36.25574111938476562500 |
| 19 | 54.60493564605712890625 | 39.02597427368164062500 | 50.33121109008789062500 | 39.95273113250732421875 | 40.77179431915283203125 |
| 20 | 55.45911788940429687500 | 39.07322883605957031250 | 49.81117248535156250000 | 39.10448551177978515625 | 39.74678516387939453125 |
| Ratio | 2.64313340187073 | 1.86949372291565 | 2.3785662651062 | 1.87021851539612 | 1.89894199371338 |



1. Performance Comparison:

- **CTR, GCM and ECB** consistently shows the fastest encryption times.
- **CBC** has moderate performed.
- **CFB** has least performances.

2. Scalability:

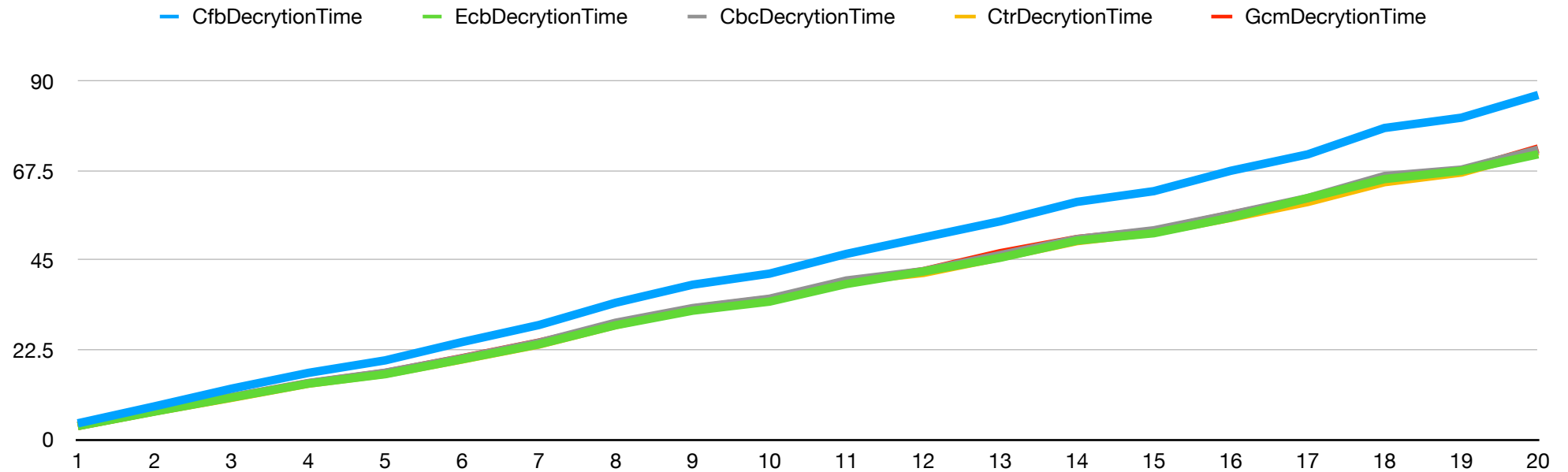
- All modes show an increasing trend in encryption time as the size increases, which is expected. However, the rate of increase varies:
 - **CFB** has a ratio about 2.64313340187073
 - **ECB** has a ratio about 1.86949372291565
 - **CBC** has a ratio about 2.3785662651062
 - **CTR** has a ratio about 1.87021851539612
 - **GCM** has a ratio about 1.89894199371338

3. Time Efficiency:

- At the 20 MB size, the encryption times are about CFB: 55.46 ms, ECB: 39.07 ms, CBC: 49.81 ms, CTR: 39.10 ms and GCM: 39.75 ms.
- Base on the performance of the time consuming, ECB, CTR and GCM not only perform faster overall but also remain more efficient with larger data sizes.

Decryption: The decryption time data is based from various algorithms (AES_CFB, AES_ECB, AES_CBC, AES_CTR, AES_GCM) across multiple sizes (1 MB to 20 MB) and time consuming are in millisecond.

| | CfbDecryptionTime | EcbDecryptionTime | CbcDecryptionTime | CtrDecryptionTime | GcmDecryptionTime |
|----|-------------------------|-------------------------|-------------------------|-------------------------|-------------------------|
| 1 | 3.95860671997070312500 | 3.26883792877197265625 | 3.31509113311767578125 | 3.26879024505615234375 | 3.30953598022460937500 |
| 2 | 8.24098587036132812500 | 6.91967010498046875000 | 7.05347061157226562500 | 6.97710514068603515625 | 6.99863433837890625000 |
| 3 | 12.69109249114990234375 | 10.44661998748779296875 | 10.56625843048095703125 | 10.36865711212158203125 | 10.50789356231689453125 |
| 4 | 16.66579246520996093750 | 13.94813060760498046875 | 14.11218643188476562500 | 13.94422054290771484375 | 14.03982639312744140625 |
| 5 | 19.81182098388671875000 | 16.33210182189941406250 | 16.70060157775878906250 | 16.42098426818847656250 | 16.64392948150634765625 |
| 6 | 24.42357540130615234375 | 20.07508277893066406250 | 20.31764984130859375000 | 20.03741264343261718750 | 20.36938667297363281250 |
| 7 | 28.71189117431640625000 | 23.85818958282470703125 | 24.25258159637451171875 | 23.79734516143798828125 | 24.29296970367431640625 |
| 8 | 34.32612419128417968750 | 28.66320610046386718750 | 29.30169105529785156250 | 28.71565818786621093750 | 28.78565788269042968750 |
| 9 | 38.86392116546630859375 | 32.32429027557373046875 | 32.97429084777832031250 | 32.75332450866699218750 | 32.84351825714111328125 |
| 10 | 41.65019989013671875000 | 34.60359573364257812500 | 35.33363342285156250000 | 34.73539352416992187500 | 35.21218299865722656250 |
| 11 | 46.62413597106933593750 | 39.04304504394531250000 | 39.92657661437988281250 | 39.69826698303222656250 | 39.43159580230712890625 |
| 12 | 50.74388980865478515625 | 42.19150543212890625000 | 42.26882457733154296875 | 41.81265830993652343750 | 42.26164817810058593750 |
| 13 | 54.82332706451416015625 | 45.63939571380615234375 | 46.31767272949218750000 | 45.75955867767333984375 | 46.79756164550781250000 |
| 14 | 59.71145629882812500000 | 49.96218681335449218750 | 50.34096240997314453125 | 49.82292652130126953125 | 50.36263465881347656250 |
| 15 | 62.41502761840820312500 | 51.82273387908935546875 | 52.56254673004150390625 | 52.01821327209472656250 | 52.36389636993408203125 |
| 16 | 67.54236221313476562500 | 55.75556755065917968750 | 56.49886131286621093750 | 55.70015907287597656250 | 56.45041465759277343750 |
| 17 | 71.66724205017089843750 | 60.67051887512207031250 | 60.67271232604980468750 | 59.67402458190917968750 | 60.37969589233398437500 |
| 18 | 78.31742763519287109375 | 65.45758247375488281250 | 66.22371673583984375000 | 64.66815471649169921875 | 65.39957523345947265625 |
| 19 | 80.90987205505371093750 | 67.54772663116455078125 | 67.83642768859863281250 | 67.09089279174804687500 | 67.50791072845458984375 |
| 20 | 86.62459850311279296875 | 71.69263362884521484375 | 72.85742759704589843750 | 72.48027324676513671875 | 73.15814495086669921875 |



1. Performance Overview:

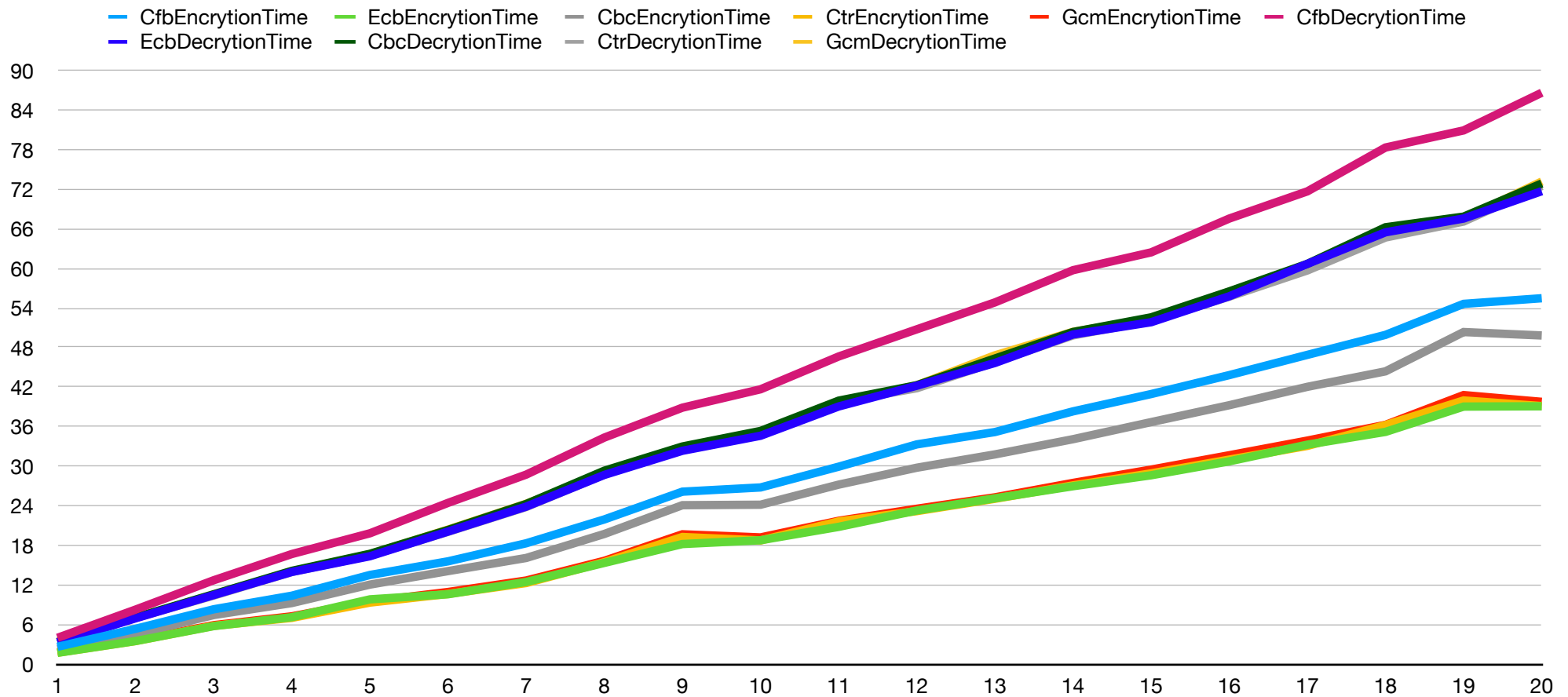
- **ECB, CTR, CBC** and **GCM** have the fastest decryption times overall.
- **CFB** has the slowest decryption time.

2. Scaling Behavior:

- All algorithms exhibit an increasing trend in decryption time as data size increases, which is expected.
 - **CFB** has a ratio about 4.1332995891571
 - **ECB** has a ratio about 3.42118978500366
 - **CBC** has a ratio about 3.47711682319641
 - **CTR** has a ratio about 3.46057415008545
 - **GCM** has a ratio about 3.4924304485321

3. Time Efficiency at 20 MB:

- At 20 MB, the decryption times are approximately about CFB: 86.62 ms, ECB: 71.69 ms, CBC: 72.86 ms, CTR: 72.48 ms and GCM: 73.16 ms.
- Base on the performance of the time consuming, ECB, CBC, CTR and GCM not only perform faster overall but also remain more efficient with larger data sizes.



Conclusion: As the figures shown, time consuming more as the data size increases. This is expected. On overall, ECB, CTR and GCM performance don't have much difference. ECB is insecure against EVA, CPA and CCA. CTR is secure against EVA and CPA. GCM is secure against EVA, CPA and CCA. Due to the performance and security, CTR and GCM would be recommended. CFB takes most of the time for encryption and decryption. One of the possible reason would be CFB is more like a stream cipher than the other four modes. This would be probably the reason why CFB has the highest cost. CTR and GCM have the best performance overall is quite surprising, because CTR and GCM have some extra step need to do compare to ECB and CBC. One of the probably reason is that the encryption and decryption process is not strongly dependent on the previous messages block. Another probably reason would be that the hardware has done some optimized processing. All tasks is performed on Apple Silicon M3 Max, which have provided the AES-IN. All the key, iv and none are prepare in advance. Only the encryption processing time and decryption processing time are in counter.