Factoring large composite numbers into its prime factors has long been a goal of mathematicians. While several methods do exist with a variability in the degree of success, no definitive way has emerged as superior to all for factoring each number. Rather, different cases requires different factoring methods. As one can see, each of the three factoring methods discussed, Trial Division, Pollard's Rho and Pollard's P-1, all have their own unique strengths and weaknesses. Trial Division, for example, takes longer than both Pollard's Rho and Pollard's P-1, however it yields more results. Many other methods also exist, and many more are currently in development. Obviously, the need for factoring still remains, and it will still remain a "prime" goal of many mathematicians.

Pros
- Cons
- Conclusion

Other Factoring Methods...
- Random square factoring
- Quadratic sieve factoring
- Number field sieve factoring

References
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography

Factoring & Cryptography

Factoring large composite numbers into its prime factors has long been a goal of mathematicians. While several methods do exist with a variability in the degree of success, no definitive way has emerged as superior to all for factoring each number. Rather, different cases requires different factoring methods. As one can see, each of the three factoring methods discussed, Trial Division, Pollard's Rho and Pollard's P-1, all have their own unique strengths and weaknesses. Trial Division, for example, takes longer than both Pollard's Rho and Pollard's P-1, however it yields more results. Many other methods also exist, and many more are currently in development. Obviously, the need for factoring still remains, and it will still remain a "prime" goal of many mathematicians.