Do zbudowania takiego szyfru posłużono się teorią liczb. Oto nieskomplikowane twierdzenie: *Jeżeli liczba naturalna N jest iloczynem dwu liczb pierwszych p, q, to dla* $M = (p-1)(q-1)+1$ *i dla każdego* $n < N$ *zachodzi*

$$n^M \equiv n \pmod{N};$$

tj. n^M i n dają z dzielenia przez N tę samą resztę.

Każda z osób, chcących mieć własny szyfr, wybiera sobie dwie dość duże liczby pierwsze (co najmniej kilkudziesięciocyfrowe) p, q, oblicza ich iloczyn N, oraz liczbę $M = (p-1)(q-1)+1$. Do wiadomości ogólnej podaje N i pewien dzielnik liczby M, oznaczmy go przez K. Dla siebie zachowuje rozkład N na p i q oraz liczbę M.

Gdy nadawca **NAD** chce wysłać wiadomość do odbiorcy **ODB**, postępuje tak. Zamienia tekst słowny na ciąg cyfr w jakiś standardowy, ustalony i jawny sposób, np. A = 1, B = 2 itd. Otrzymaną tak dużą liczbę (komunikat nie może być długi) podnosi do potęgi K_{ODB} i bierze resztę z dzielenia przez N_{ODB}. Potrzebna jest do tego maszyna matematyczna, ale nic ponadto. Tak zakodowaną wiadomość (będącą teraz liczbą mniejszą niż N_{ODB}) wysyła się do odbiorcy lub publikuje w gazecie. Odbiorca winien podnieść tę liczbę do potęgi $\frac{M_{ODB}}{K_{ODB}}$ — otrzyma wtedy ciąg liczb wysłany przez nadawcę. Przetworzenie go na tekst słowny odbywa się we wspomniany jawny i standardowy sposób.

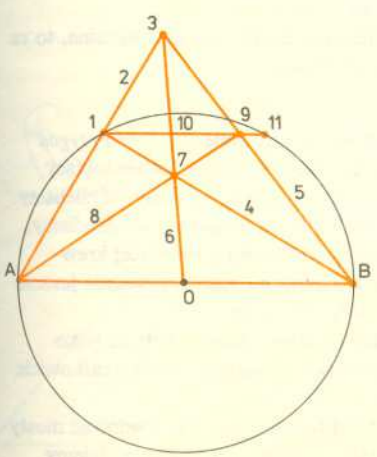
Co w tym takiego rewelacyjnego? — zapytacie. A to, że podniesienie nawet bardzo dużej liczby do bardzo dużej potęgi M jest dla maszyny matematycznej mało pracochłonne, zwłaszcza że wszystkie obliczenia robi się i tak modulo N. Wynik dostaje się w ułamku sekundy. Osoba postronna nie zna jednak liczby M; mogłaby ją obliczyć, znając p i q. Ale zna tylko N, równe pq. Gdy p i q mają po kilkadziesiąt cyfr, N ma sto kilkadziesiąt. Znalezienie rozkładu takiej liczby na czynniki nawet najszybciej działającej maszynie zajęłoby (przy obecnym stanie techniki, informatyki i organizacji maszyn cyfrowych) wiele, wiele lat pracy.

Szyfr ten nie daje się złamać najgroźniejszą bronią: analizą statystyczną, rozpracowującą szybko wszystkie szyfry polegające na stałym przyporządkowaniu litera-liczba. Autorzy tego szyfru napisali (w *Scientific American*), że są niezbicie pewni, iż nikt nie potrafi odczytać zaszyfrowanej przez nich do samych siebie wiadomości.

Tylko linijką

Jeżeli mamy na kartce papieru narysowany okrąg z zaznaczonym środkiem O, to możemy bez trudu samą linijką wpisać w ten okrąg kwadrat. Robi się to w następujący sposób (rysunek podzieliliśmy na dwa etapy): Prowadzimy dowolną średnicę. Jej końce oznaczamy A i B. Obieramy na okręgu jeszcze jeden punkt *1*. Na prostej *2* przechodzącej przez A i *1* obieramy na zewnątrz okręgu punkt *3*. Łączymy *1* z B prostą *4*, *3* z B prostą *5* i *3* z O prostą *6*. Przez punkt *7* leżący na prostych *4* i *6* prowadzimy prostą *8* do przecięcia z *5* w punkcie *9*. Prosta *10* łącząca *1* i *9* przecina okrąg w punkcie *11*. Przez B i *11* prowadzimy prostą *12* do przecięcia z *2* w punkcie *13*. Prosta *14* łącząca O i *13* przecina okrąg w punktach C i D. Czworokąt $ACBD$ jest kwadratem, co Czytelnik z łatwością udowodni wykazując, że prosta *10* jest równoległa do AB (pierwszy rysunek), zaś kąt AOC jest prosty (drugi rysunek).

Półtora wieku temu Steiner wykazał, że każda konstrukcja wykonalna cyrklem i linijką jest wykonalna samą linijką, o ile tylko mamy do dyspozycji (być może nawet dość daleko, ale na tej samej karcie) jeden narysowany okrąg z zaznaczonym środkiem. Można spróbować dowieść, że tak jest w istocie, lub znaleźć steinerowską konstrukcję dla jakiegoś wybranego zadania.



W okrąg z zaznaczonym środkiem można wpisać kwadrat za pomocą samej linijki