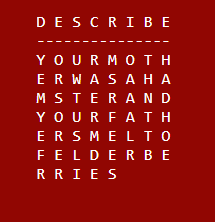
این الگوریتم که در جنگ جهانی اول توسط آلمانی ها به کار برده شد یکی از امن ترین رمزهای دستی مورد استفاده بود. هم توسط متفقین و هم توسط Axis مورد استفاده قرار گرفت و به خوبی به هر دو خدمت کرد. نقطه ضعف اصلی آن این بود که اگر مهاجم دو یا چند پیام با طول یکسان را با استفاده از کلید یکسان رهگیری کند، می‌توان آنها را با فرآیندی به نام "تشخیص چندگانه" مقایسه کرد و برای هر دو راه‌حل یافت. اگر با استفاده از هر کلید فقط یک پیام ارسال می شد، این ضعف مهم نبود. این یک مشکل اضافی داشت: اجرای صحیح آن به دقت قابل توجهی نیاز دارد و در صورت بروز خطا در نقطه حساس، رمزگشایی با مشکل مواجه خواهد شد. در ایالات متحده، اطلاعات مربوط به تحلیل رمز رمز تا چند سال پیش طبقه بندی شده بود.

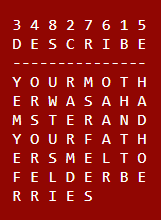
Double Transposition شامل دو کاربرد انتقال ستونی به یک پیام است. این دو برنامه ممکن است برای هر یک از دو مرحله از یک کلید استفاده کنند یا ممکن است از کلیدهای متفاوتی استفاده کنند.

روش الگوریتم double transposition ستونی :

ابتدا یک کلمه دلخواه انتخاب میشود سپس پیام اصلی ما زیر آن نوشته میشود مانند شکل زیر :

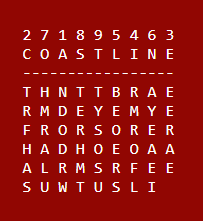


سپس بر اساس ترتیب حروف الفبا حروف کلید ترتیب بندی میشوند :

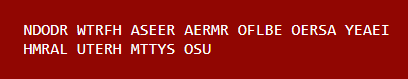


در مرحله بعدی ستون ها به ترتیب خوانده میشوند مثلا ستون اول بدین صورت است : THNTTB

بعد از آن ستون هایی که استخراج شده بود را به ترتیب با توجه به کلید دوم پشت هم مینویسیم و دوباره کلید دوم را شماره گذاری میکنیم :



و در آخر هم مشابه کلید اول cipher text بدین صورت میباشد :



برای رمز گشایی هم مراحل انجام شده را برعکس انجام میدهیم یعنی یک بلوک با تعداد ردیف های مناسب زیر کلمه کلیدی بسازید و ستون های کوتاه را مسدود کنید. رمز را به صورت ستونی بنویسید و آن را با سطر بخوانید.