Cursus Cryptografie

Purple

17–02-2016


VIDEO

Tijdlijn

- 1919 Yardley sticht American Black Chamber
- 1921 Gebroken codes vlootconferentie
- 1929 Black Chamber gesloten
- 1930 Japanse Red machine
- 1931 Yardley publiceert *The American Black Chamber*
- 1939 Purple in Japanse ambassades operationeel
- 1940 Friedman c.s. breken Purple

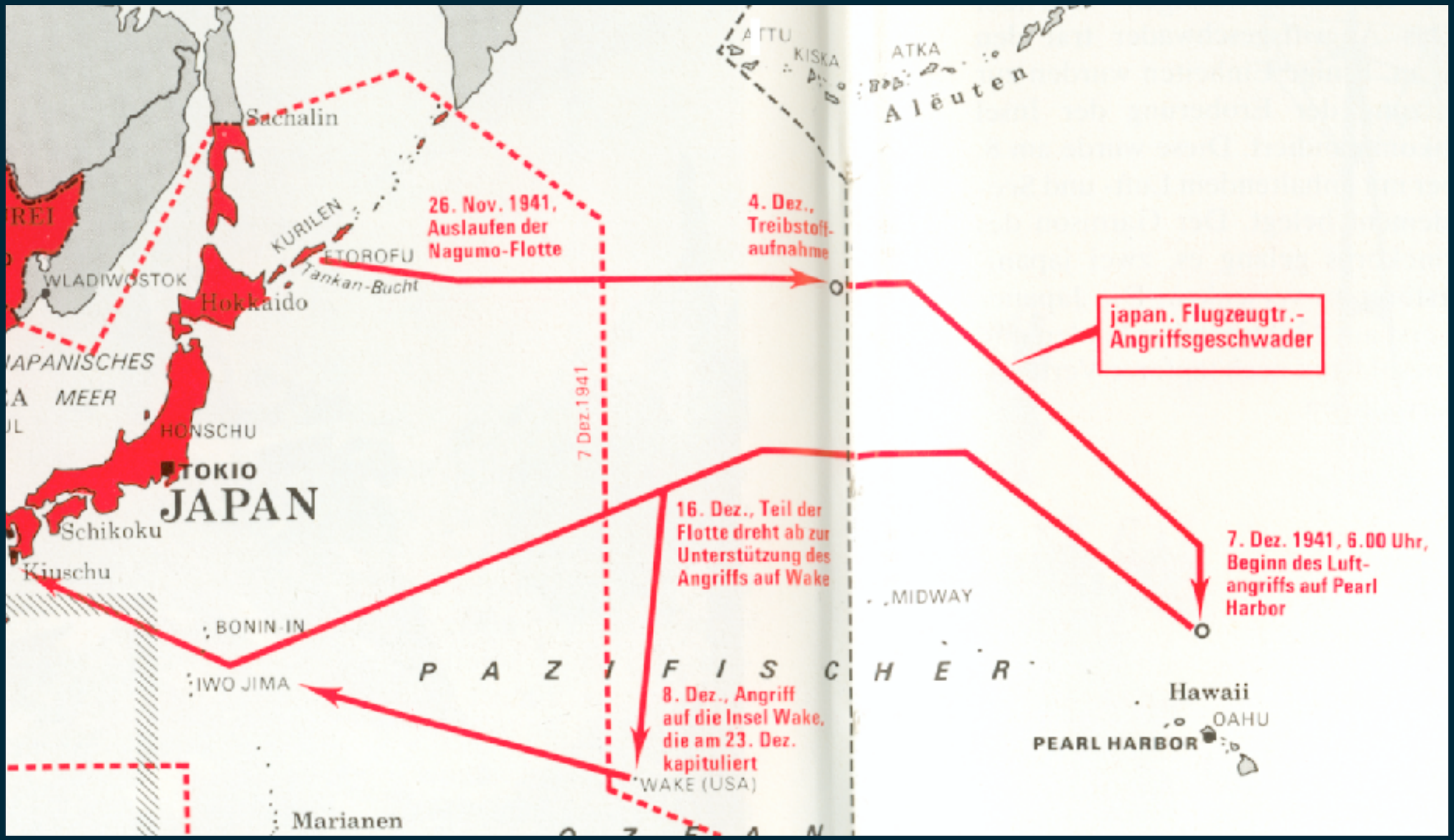
Japans “ultimatum”

- eind 1941 onderhandelingen Japan-USA
- Japans kabinet besluit tot oorlog
- artikel 1 uit Verdrag van Den Haag 1907

  … hostilities … must not commence without previous and explicit warning, in the form of either a reasoned declaration of war or of an ultimatum with conditional declaration of war.

- Japans kabinet besluit waarschuwingstijd uiterst kort te houden

Aanval op Pearl Harbour



Instructie ambassade

From: Tokyo

To: Washington

December 7, 1941

Purple (Urgent - Very Important)

#907. To be handled in government code.

Re my #902.

Will the Ambassador please submit to the United States Government (if possible to the Secretary of State) our reply to the United States at 1:00 p.m. on the 7th, your time.

1:30 PM Washington = 8:00 AM in Pearl Harbour, Hawaii

14e deel Purple decrypt

Tokio verstuurt dit deel pas op het allerlaatste moment naar de ambassade in Wahington

Obviously it is the intention of the American Government to conspire with Great Britain and other countries to obstruct Japan's efforts toward the establishment of peace through the creation of a New Order in East Asia, …

The Japanese Government regrets to have to notify hereby the American Government that in view of the attitude of the American Government it cannot but consider that it is impossible to reach an agreement through further negotiations.

Japanse ambassade

- 3 december 1941
  bevel op 1 na alle codeermachines vernietigen
- 6 december 1941
  voor het diner 13 van 14 delen ontvangen
  - afscheidsfeest vertrekkende collega
  - om middernacht alle 13 ontcijferd
  - opdracht bericht vast gereedmaken genegeerd
- nacht 6 op 7 december 1941
  deel 14 + overhandigingsinstructie lopen binnen

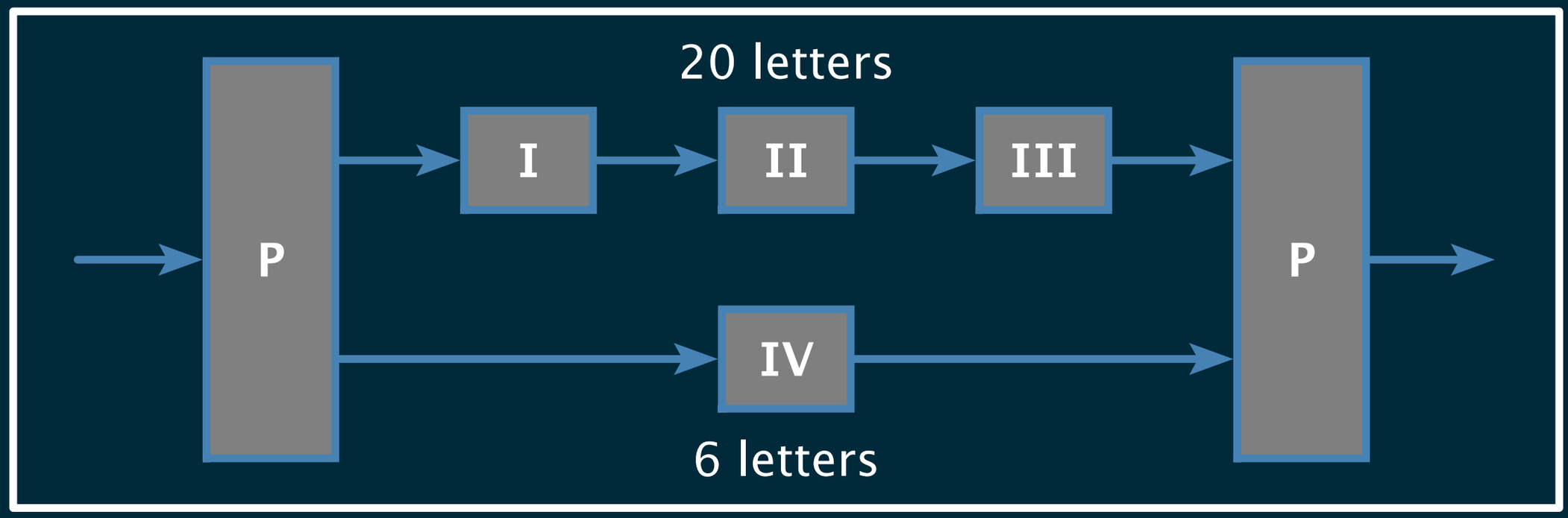
Ramp voltrekt zich

- 7 december 1941 09:30 uur
  decoderen van de post begint
- 11:30 uur overhandigingsinstructie gedecodeerd
  overhandiging om 13:00 uur
  deel 14 is nog niet gedecodeerd
- 12:30 deel 14 gedecodeerd gereedmaken traag
- ambassadeur stelt overhandiging uit tot 13:45
- 13:25 eerste aanvalsgolf boven Pearl Harbour
- 14:05 overhandiging Japanse “oorlogsverklaring”

Red machine

- klinkers naar klinkers 6x6 Vigenère
- medeklinkers 20x20 Vigenère
- progressie 24x(1)(2)13x(1)(2)
- 1935-1936 cryptoanalyse Signal Intelligence Service
- 1938 cryptoanalyse Pers-Z (BuZa Duitsland)
- allerbelangrijkst: 6x6 scheiding voortgezet in Purple

Purple mechanisme

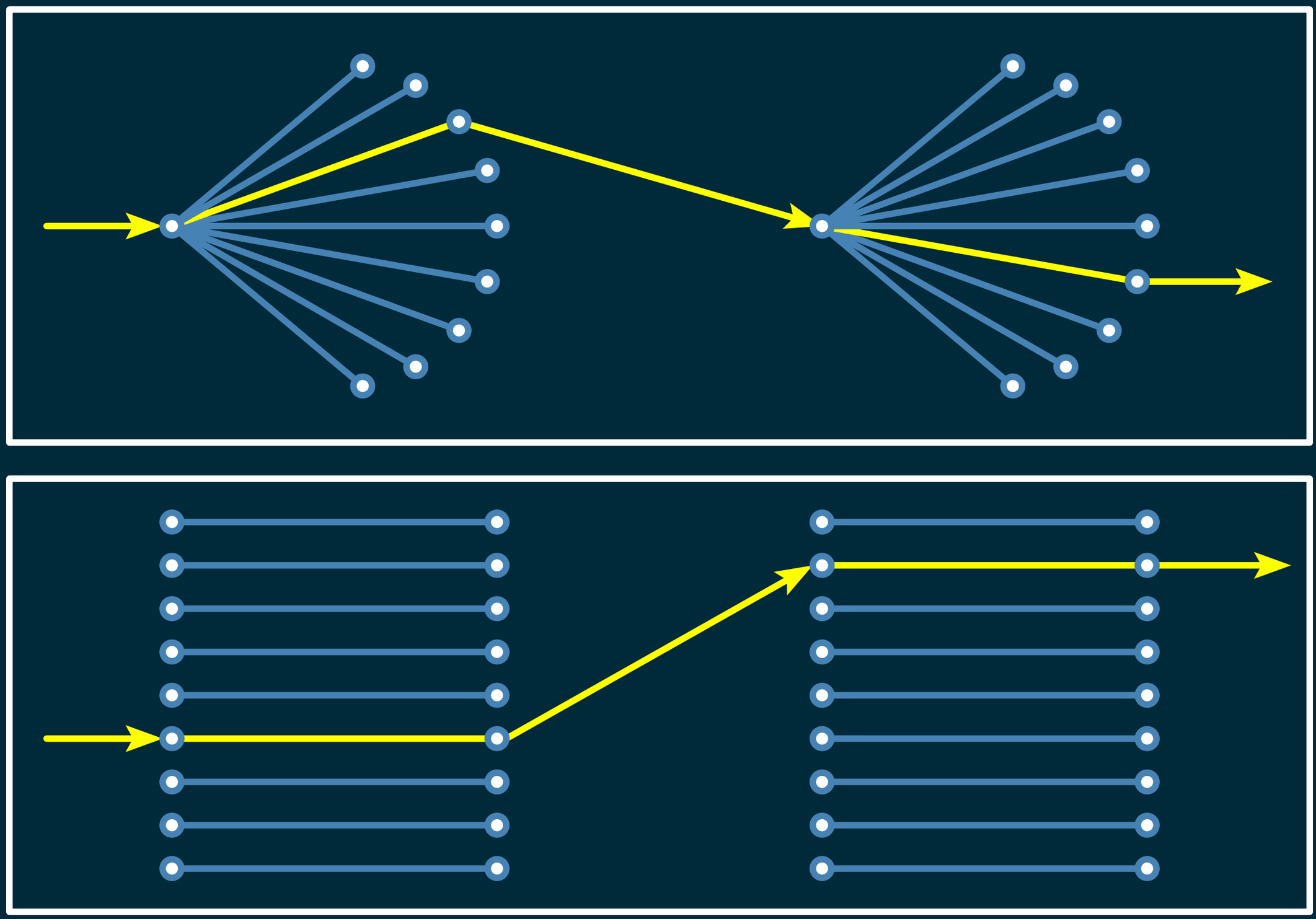


P = Plugboard

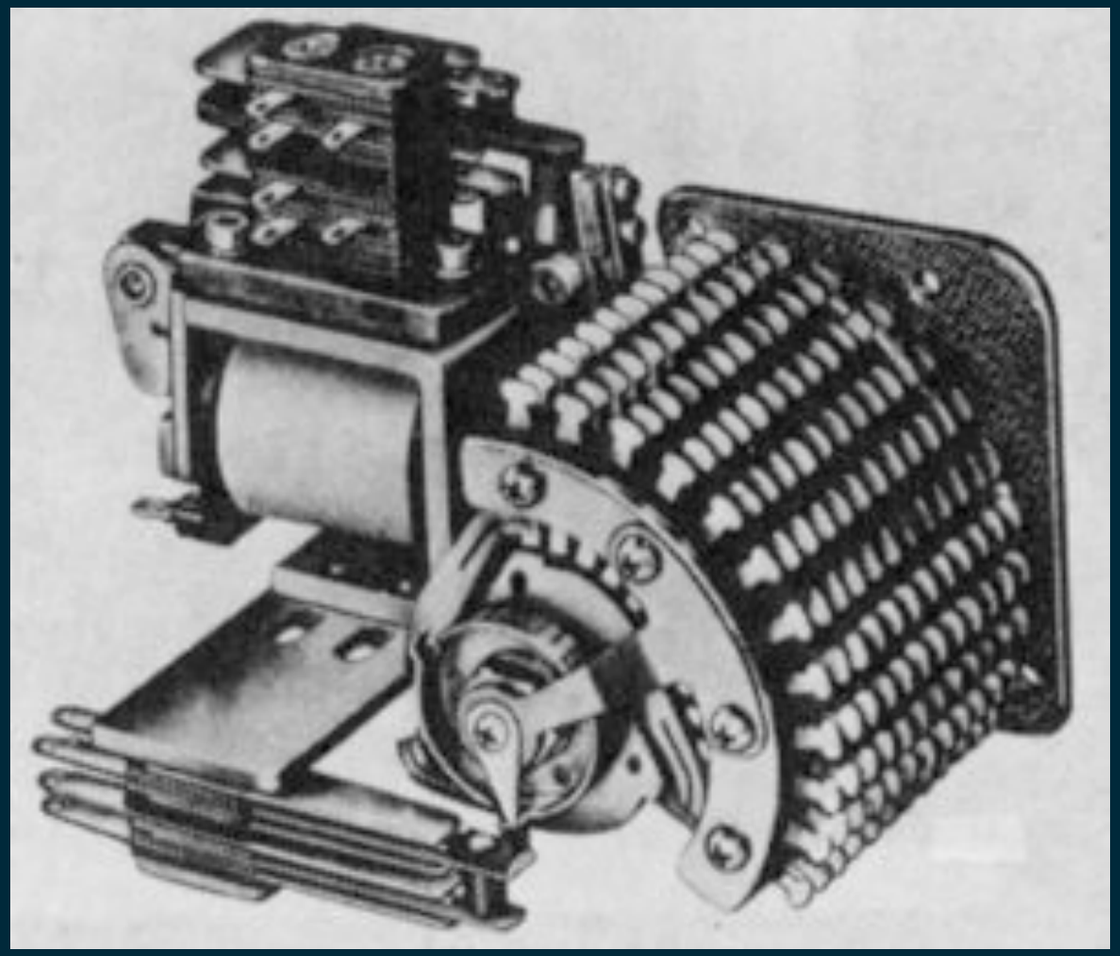
I, II, III = 20 letters 25 subsituties Fast - Medium - Slow

IV = 6 letters 25 substituties

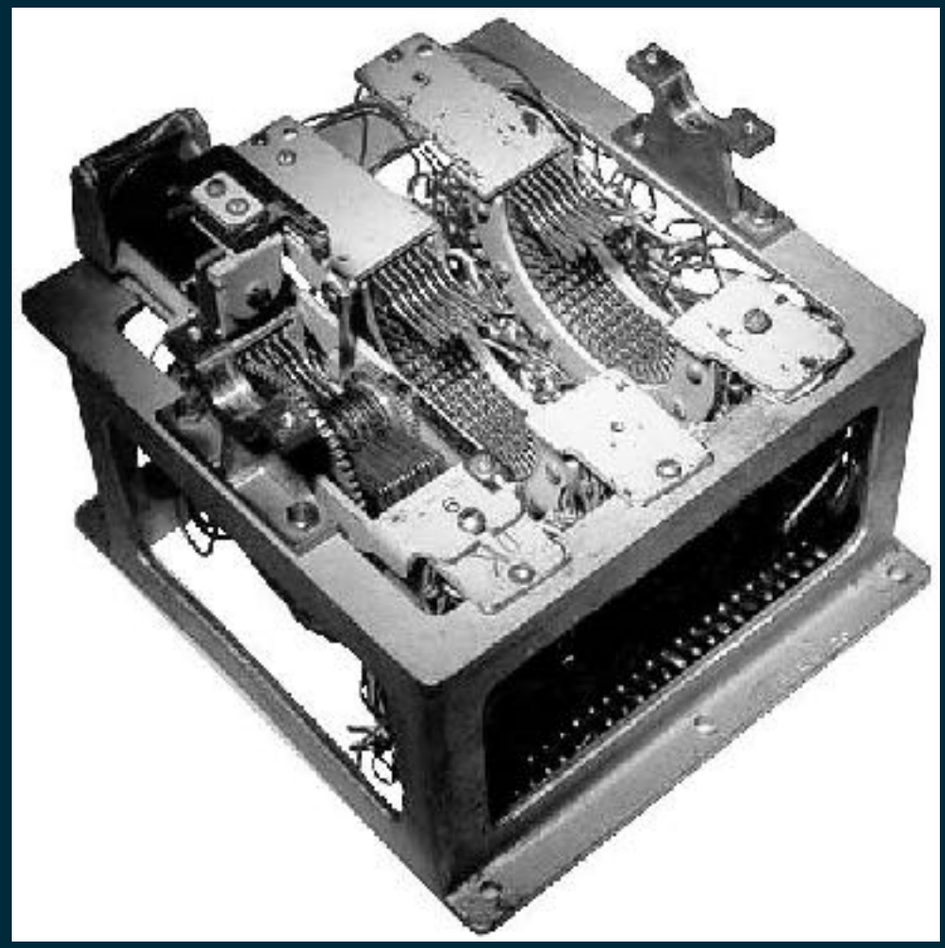
Purple substitutie



Techniek



stappenschakelaar



purple restant

Cryptoanalyse

- 1939 marine en leger in team Friedman
- 6/20 klinker-medeklinker van Red blijkt gehandhaafd
- klinkers in Romaji variant Japans zeer frequent
- Purple geleidelijk naast Red → isologe berichten
- Leo Rosen stappenschakelaar implementatie
- door isomorfie collectie substituties te completeren
- identificatie FMS uit verschillend substitutie patroon
- analyse bericht indicatoren voor instelling machine

Resultaat

Memo van William Friedman
14 oktober 1940

Credits o.a. Frank Rowlett, Samuel Snyder, Leo Rosen, Abraham Sinkov, Genevieve Grotjan

Friedman

Grotjan

Rowlett

Sinkov

Beginstap

- identificeer de groep van 6 letters
  niet meer alleen klinkers dankzij plugboard

```
BRAXEFQCEVQOOXHECFDLNHQRVQPPLCERP...
 HE A A E E   ER  E  REQ E    HA ...
```

- bepaal de 6 → 6 substituties

- completeer de tekst door interpolatie

```
BRAXEFQCEVQOOXHECFDLNHQRVQPPLCERP...
 HE A A E E   ER  E  REQ E    HA ...
THEJAPANESEGOVERNMENTREQUESTSTHAT...
```

Echt bericht

code: XFCGJ WFOVD DNOBB FYXFO CFYLC CFMSG TSJVR

```
XFC = Dai-go                    MS   = 3
GJW = 15                        GTS  = Getsu (month)
FOV = (                         JVRK = Juroku (16th)
DD  = 2                         HI   = day
NO  = of                        FIC  = begin kana
BB  = 1                         GURV = Guru (Grew)
FYX = )                         FEL  = end kana
FOC = Gokuhi (secret)           BKW  = Beikoku (U.S.)
FYL = Kancho fugo atukai        TLSI = Taishi (Ambassador)
CCF = Shin sho (paragraph)
```

Number 15 (part 1 of 2 parts) Secret, to be kept within Department
§ On March 16th the U.S. Ambassador, Grew …

Analyse

- beschikbaar 1000+ berichten
  waarvan 15 lang (± 1500 letters)
  zowel Japanse als Engelse teksten
- geen echte herhalingen dus periode > 1500
  minder herhalingen dan random verwachting
- zelfde dag zelfde indicator → Kerckhoffs
- te weinig voor oplossing daarom conversie
  tussen berichten met verschillende indicator
- door conversie 6 berichten voor Kerckhoffs

Tijdtabel

- 20 september 1940
  Grotjan spot de eerste herhalingen
  substituties gereconstrueerd
  reductie substituties tot bedrading
- 27 september 1940
  2 berichten opgelost
- 14 oktober 1940
  een kwart van de indicatoren opgelost
- resteert elke dag nieuwe plugboardinstelling

Isomorfie

input contact

	A	B	C	D	E
119			D		
120					D
121	D				
122				D	
123		D			
124			B		
125					B
126	B				
127					
128		B			
129					
130					A
131					
132				A	
133		A			

	A	B	C	D	E
119			D		
120					D
121	D				
122				D	
123		D			
124			B		
125					B
126	B				
127				B	
128		B			
129			A		
130					A
131	A				
132				A	
133		A			

Literatuur

- W.F. Friedman (1940) Preliminary Historical Report on the Solution of the "B" Machine
- D. Kahn (1967) The Codebreakers – One Day of MAGIC
- C.A. Deavours, L. Kruh (1985) Machine Cryptography and Modern Cryptanalysis
- W. Freeman, G. Sullivan, F. Weierud (Cryptologia 2003) Purple Revealed: Simulation and Computer-Aided Cryptanalysis of Angooki Taipu B