



Co-funded by
the European Union



Разбивачи на кодове Мидуей

Битката за Midway 3-7 юни 1942

This project has received funding from the **DIGITAL-2021-QCI-01 Digital European Programme** under
Project number No 101091399.

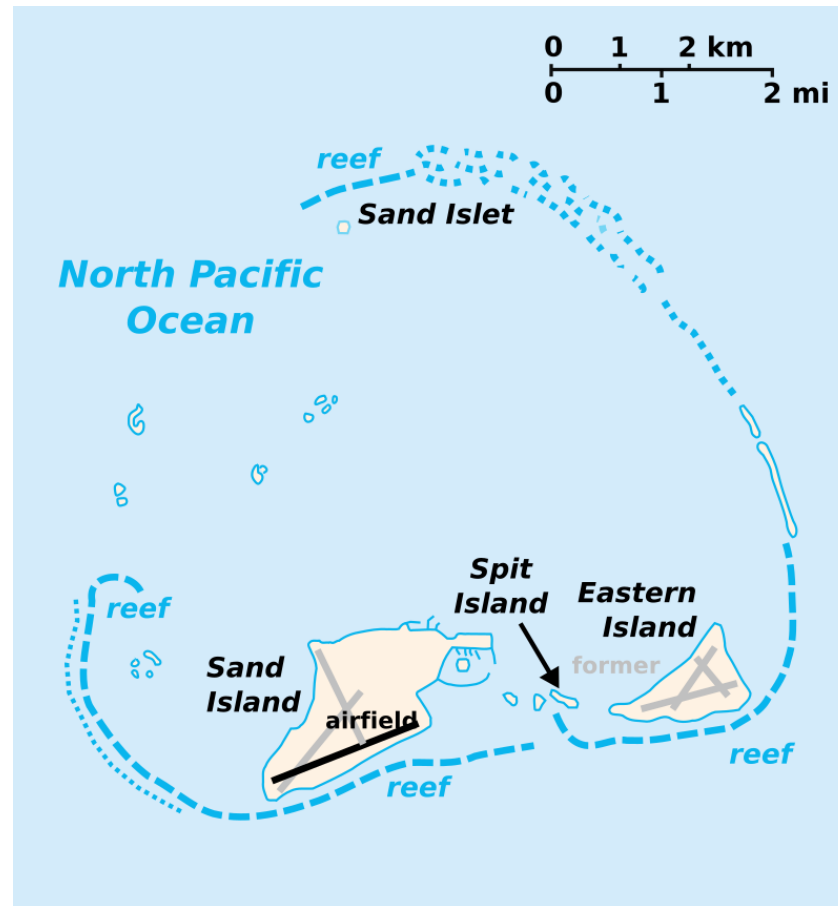
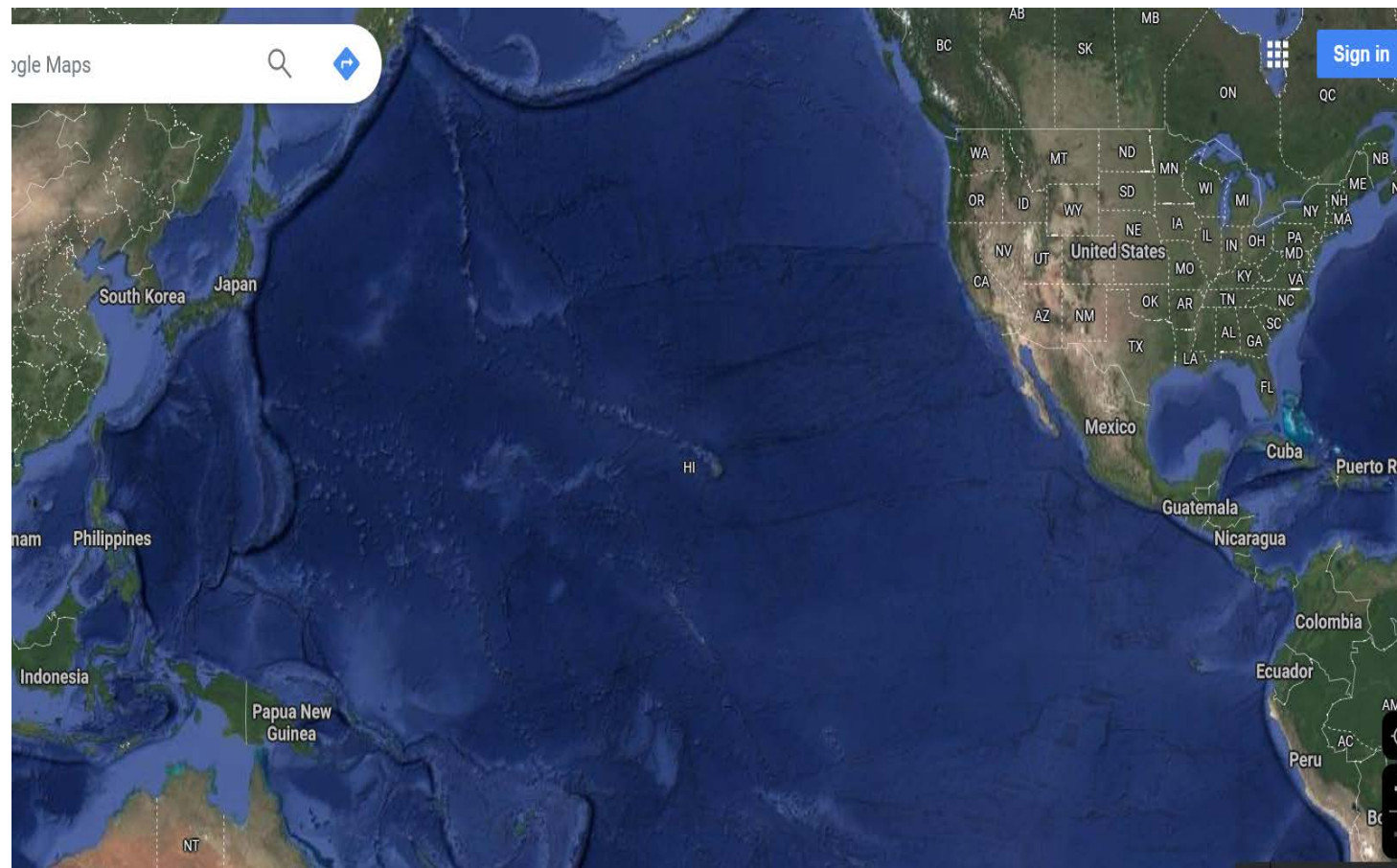
OCTOBER 2024

МЕСТОПОЛОЖЕНИЕ на атола в Тихия океан:

С HI на лявата карта са обозначени Хавайските острови;

Мидуей е на около 2100 км на северозапад от Хонолулу.

(Разстоянието между Сан Франциско и Токио е около 8270 км.)



The Red Book

陸軍暗號書四號

參謀本部

8500	8533 顔紫な	8567 「ローマ」(羅馬)
8501 K	8534 「スマラン」	8568 獨立守備隊の
8502 陸軍部の中隊の	8535 陸軍部の中隊の	8569 陸軍部の中隊の
8503 ナツ	8536 ナツ	8570 参謀部長の
8504 朝 鮮	8537 山 崎 府	8571 何 應 欽
8505 沿 道	8538 便 本	8572 名 稱
8506 當院の	8539 敵 艇	8573 眞 性 本
8507 恰 毛	8540 (ノ)見込ナ	8574 治 察 士
8508 功〇級	8541 幹部候補生	8575 即 日
8509 指揮官	8542 不安な	8576 電 報 報 示
8510 遺 囑 ナ	8543 十九時	8577 手段ヲ明
8511 手配中な	8544 發 示	8578 要
8512 「ワスタ	8545 「マヅク」島	8579 第十一師隊の
カムナツカ	8546 船匠工員	8580 岡 崎
8513 二 宮	8547 カ 船〇艦隊の	8581 ス デ
8514 ハ ネ	8548 金 部	8582 陸軍機甲整備學校
8515 蒙 古	8549 協議し	8583 傳ヘラル
8516 南方地区の	8550 ナット思考し	8584 近 (シ、ア)
8517 部 内	8551 駐 劄	8585 第〇部隊の
8518 當司令部の	8552 附 属	8586 海 支
8519 檢學し	8553 洩出し	8587 スルトコロ
8520 監禁し	8554 07	8588 入 湖
8521 相當(ニ)	8555 發信者(名)	8589 電 報 第 〇 號
8522 獸醫部の	8556 印度支那	8590 航 空 密 電 第 〇 號
8523 約〇杆	8557 青 木	8591 第〇師隊の
8524 福 岡	8558 コ ル	8592 旅 客 機 の
8525 三十分	8559 永 興 海	8593 Ⅲ(彙字)
8526 新 郷	8560 塙 浩	8594 火 炮 發 射 器
8527 武 通 し	8561 射 擊 彈	8595 陸 軍 燃 料 廠
8528 高級副官の	8562 密 偵 報 = 依 (ルニレバ)	8596 後 續 師 隊 の
8529 空地連絡	8563 優 勢 な	8597 資 源 の
8530 出發(ヲ)準備し	8564 連 絡 者 の	8598 コ ト ト
8531 部 下	8565 作 井	
8532 慰問袋	8566 九七式	

От японски към числа

	<i>Rōmaji</i>		<i>Nippongo</i>
	<i>Telegraph</i> <i>(Millikin)</i>	<i>Literary</i> <i>(Holden)</i>	<i>Literary</i> <i>(Millikin)</i>
A.....	98	183	141
B.....	6	7	10
C.....	2	6	0
D.....	16	20	25
E.....	56	61	51
F.....	5	3	0
G.....	16	13	26
H.....	35	45	10
I.....	112	125	101
J.....	2	2	0
K.....	66	52	79
L.....	0	0	0
M.....	31	54	35
N.....	72	68	88
O.....	154	123	142
P.....	6	2	10
Q.....	0	0	0
R.....	41	39	48
S.....	49	65	29
T.....	45	76	68
U.....	75	39	58
V.....	0	0	0
W.....	23	25	30
X.....	0	0	0
Y.....	51	9	14
Z.....	9	3	7
Total.....	970	1000	972

JN-25b Imperial Japan Navy's Command and Control Code (manual encoding)

	001								
0	25751	04625	76730	80641	46476	78249	29212	17948	4
1	80663	32414	26123	95202	24375	80324	49248	93580	7.
2	13648	79304	56253	16912	84214	43020	98512	24179	;
3	08375	26559	97476	59075	72565	37675	14959	61290	;
4	36875	86331	15307	20354	97835	64973	37290	95760	4
5	74070	23621	86409	02279	13201	86171	07124	48373	7
6	58963	72714	17063	59323	76451	46075	19606	83695	2.
7	93559	48051	72397	69752	32610	02431	23287	58590	39:
8	63908	50519	30479	73626	29589	35035	41187	12841	68

Additives: събиране без 1 наум

(呂貳ノ三)												
072												
	91	50	24	73	56	39	02	15	44	81	54	70
16	14929	35628	80562	00147	88137	93504	21580	58865	97820	17326	58553	01076
55	23183	63454	07541	65826	38803	42393	94004	78478	04047	33917	36748	52211
32	36831	78346	37569	43223	01494	14713	46236	32552	58667	91712	08545	94070
17	71819	48704	11557	81078	90567	25006	84864	67611	40964	47620	97947	17795
98	61324	58431	96434	33724	57592	75904	54976	16316	30250	52377	49357	06013
05	44635	95083	21137	67209	29321	98312	06037	89563	74978	00156	87674	34542
33	53252	04722	58423	82158	76806	49301	39186	77288	20120	72090	15782	63648
95	97453	22039	61220	56471	41787	34328	78153	46194	85468	25594	78568	28030
07	84961	70850	44526	18789	60024	54267	10645	09150	62621	65227	16912	93190
52	02813	83298	74802	03172	15648	26854	02163	92218	13055	84914	64117	11285
46	85513	62153	95276	31374	06282	80818	63245	36022	86083	45706	08607	71953

Разбивачи на кодове

- Joseph John Rochefort and Huro (Pearl Harbor)
- AF: Целта на японския флот е Midway
- Датата: 3 юни 1942 (декодирани JN-25 шифрограми)
- Засадата на Адмирал Chester Nimitz
3 самолетоносача, 45 бойни кораби и 25 подводници
на 100 км от Midway

Капитан Джоузеф Рошфорт
(Capt. Joseph J. Rochefort),
12.05.1900 - 20.07.1976,
криптоаналитик на Station
HYPO в Пърл Харбър, който
дешифрира японските
съобщения за атаката над
Мидуей



JN-25 not One-Time Pad



the superseded system had been the BLUE CODE, based on the color binding used for the American recoveries to the system; the new code was designed BLACK. The BLACK CODE introduced the use of an additive book to superencipher messages.

The BLACK CODE did not last long. The Japanese Navy introduced two new enciphered codes for general purposes in 1939; American cryptanalysts dubbed one of the systems the "Flag Officers Code" and the other, JN-25. Both systems were worked by Navy cryptanalysts, although the U.S. Navy got little intercept in the Flag Officers Code and the effort against it was abandoned in December 1941.

The Flag Officers Code was never solved by the Americans. JN-25, however, became one of the most widely used Japanese Navy systems -- and, eventually, a critical source of intelligence for the Allies.

JN-25 consisted of a codebook with approximately 27,500 entries and an additive book for superenciphering the codebook values. The additive book consisted of 300 pages, each page containing 100 random five-digit groups. It should be noted that this additive book for JN-25 was not a one-time pad: the five-digit groups were re-used, as needed.

In studying JN-25, U.S. cryptanalysts had to collate large numbers of Japanese messages over time. Their first goal was to recover the indicator in each message which showed where in the additive book numbers were taken; then recover and strip away the additives

Заклучение

- Битката за Midway е спечелена от САЩ благодарение на криптографите, криптоанализа, анализ на трафика и пеленгация
- Декодирани са не повече от 20% от съобщенията на японците
- Разбиването на шифъра JN-25b е било възможно само заради многократното използване на секретните ключове (additives)
- Японският флот е непоправимо разрушен, загубени са 4 самолетоносача, един крайцер, около 300 самолета и над 3000 пилоти.
- Американците губят 362 души, 1 самолетоносач, един разрушител и 144 самолета

Заклучение

- На 18 април 1943 г. адмирал Ямамото загива при Соломоновите острови. Самолетът му е пресрещнат и свален от американски изстребители, отново след прехващане и декодиране на секретни японски съобщения
- След Мидуей адмирал Нагумо изпада в прогресираща депресия. На 6 юли 1944 г. се самоубива с личния си пистолет под заплахата от попадане в американски плен на един от Марианските острови (о-в Сайпан)
- На 2 септември 1945 г. на борда на кораба Мисури адмирал Честър Нимиц подписва като представител на САЩ официалния документ за капитулацията на Япония