Financial Cryptography in the Telegraph Era

Steven M. Bellovin
http://www.cs.columbia.edu/~smb

A Typical Entry (1882)

Identity can be established if the party will answer that his or her mother's maiden name is..... } **05626 Guineapig**

- Use a single word or number to encode an entire phrase
- Primarily for economy and error detection/correction
- First telegraph codebook published in 1845; peaked in 1920s
- Could use superencipherment for confidentiality, typically by modular addition of a secret value – the key – to the code number and then selecting the new code word
- Codebooks were often domain-specific

The Federal Reserve Codebook (1921)

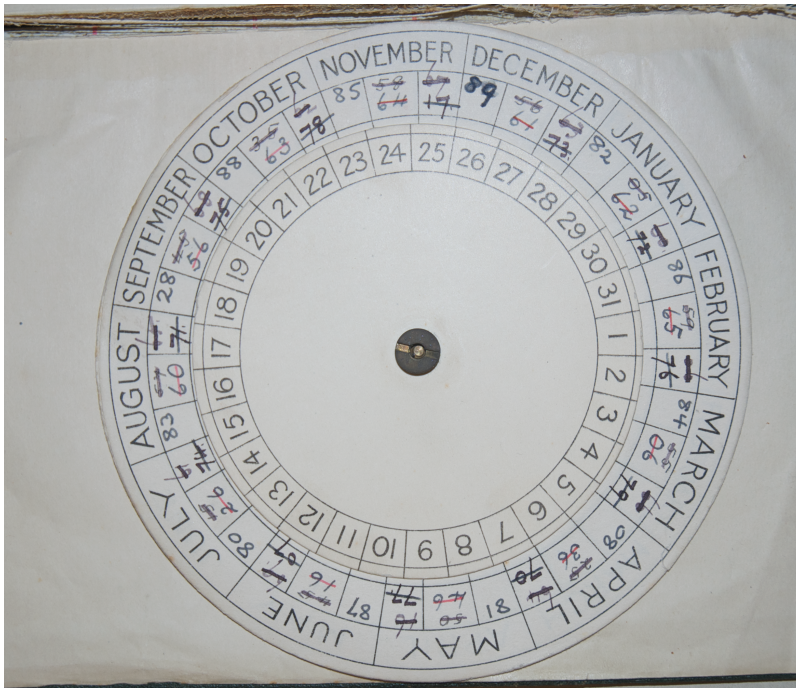
- Typical financial codebook
- Required external "test words" for authentication
- Did some of the codewords have a hidden message?

Hydrant	Sec. of Treasury
Hymen	Supt. of Banks
Hypnotism	U.S. Congress
Hypocrisy	The President
Hysterical	Treasury Dept.
Ignoramus	U.S. of America
Ignorant	U.S. Senator
Imbibing	War Department
Imbosom	White House

Authentication via Test Words

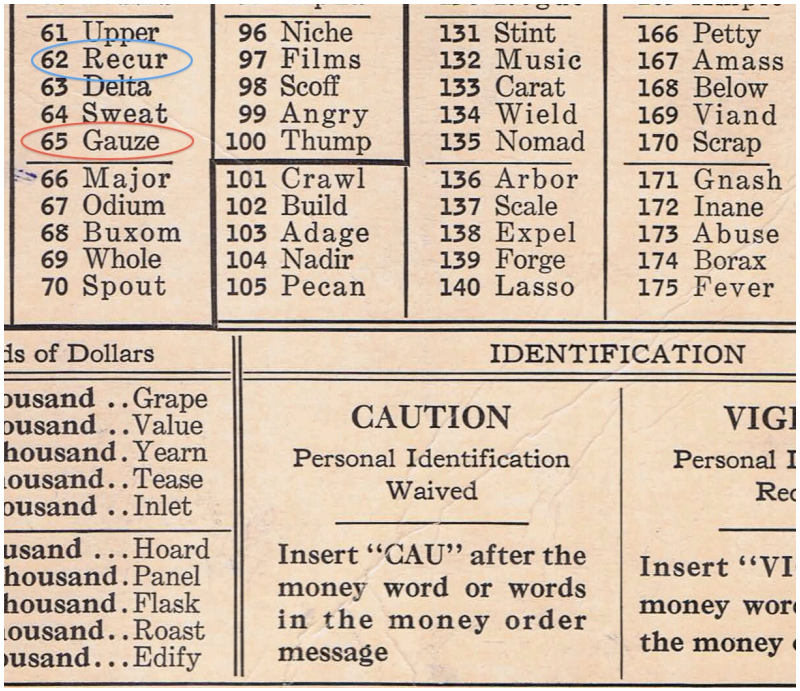
- Include a time-varying "test word"
- Phrase appears to come from secrets used to authenticate to secretive social organizations (e.g., Freemasons)
- Use in telegraphy dates to 1870s; threats include employees and poorly-paid telegraph operators
- By World War I, exemption in the censorship rules for use of test words by registered, trusted organizations

An Authentication Codewheel?



- Royal Bank of Ireland (undated; probably around 1900-1910)
- Codewheel is possibly a later addition; exact usage is unclear
- Probably intended to generate test words

Western Union Two-Part Code (1953)



61 Upper	96 Niche	131 Stint	166 Petty
62 Recur	97 Films	132 Music	167 Amass
63 Delta	98 Scoff	133 Carat	168 Below
64 Sweat	99 Angry	134 Wield	169 Viand
65 Gauze	100 Thump	135 Nomad	170 Scrap
66 Major	101 Crawl	136 Arbor	171 Gnash
67 Odium	102 Build	137 Scale	172 Inane
68 Buxom	103 Adage	138 Expel	173 Abuse
69 Whole	104 Nadir	139 Forge	174 Borax
70 Spout	105 Pecan	140 Lasso	175 Fever

ds of Dollars

ousand . . Grape
ousand . . Value
housand . Yearn
ousand . . Tease
ousand . . Inlet

usand . . . Hoard
housand . Panel
housand . Flask
ousand . . Roast
usand . . . Edify

IDENTIFICATION

CAUTION

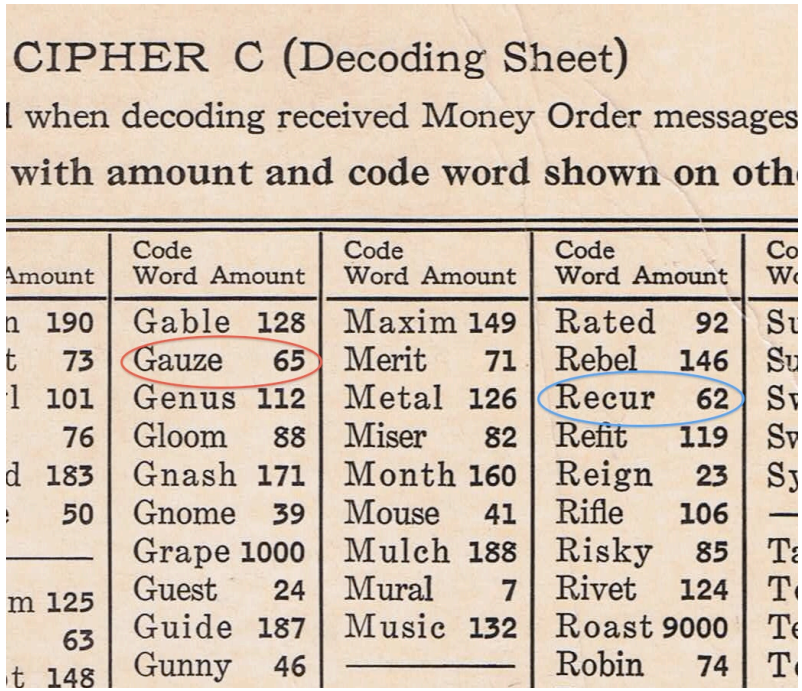
Personal Identification Waived

Insert "CAU" after the money word or words in the money order message

VIGI

Personal I
Rec

Insert "VI
money wor
the money

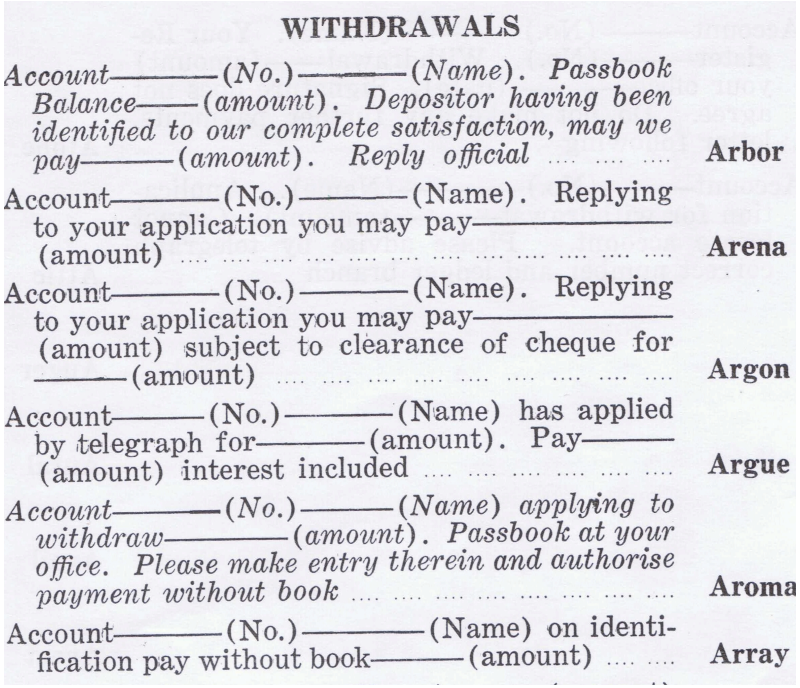


CIPHER C (Decoding Sheet)

l when decoding received Money Order messages
with amount and code word shown on oth

Amount	Code Word	Amount	Code Word	Amount	Code Word	Amount	Co Wo
n 190	Gable	128	Maxim	149	Rated	92	Su
t 73	Gauze	65	Merit	71	Rebel	146	Su
l 101	Genus	112	Metal	126	Recur	62	Sv
76	Gloom	88	Miser	82	Refit	119	Sv
d 183	Gnash	171	Month	160	Reign	23	Sy
50	Gnome	39	Mouse	41	Rifle	106	—
———	Grape	1000	Mulch	188	Risky	85	Ta
m 125	Guest	24	Mural	7	Rivet	124	Te
63	Guide	187	Music	132	Roast	9000	Te
t 148	Gunny	46	———		Robin	74	Te

A Relatively Recent Codebook



WITHDRAWALS

Account———(*No.*)———(*Name*). *Passbook Balance*——(*amount*). *Depositor having been identified to our complete satisfaction, may we pay*———(*amount*). *Reply official* .... **Arbor**

Account———(No.)———(Name). Replying to your application you may pay———— (amount) .... **Arena**

Account———(No.)———(Name). Replying to your application you may pay———— (amount) subject to clearance of cheque for ———(amount) .... **Argon**

Account———(No.)———(Name) has applied by telegraph for———(amount). Pay——— (amount) interest included .... **Argue**

Account———(*No.*)———(*Name*) *applying to withdraw*———(*amount*). *Passbook at your office. Please make entry therein and authorise payment without book* .... **Aroma**

Account———(No.)———(Name) on identification pay without book———(amount) .... **Array**

- Australian postal banking, 1968
- Note that entries can use parameters
- No provision for authentication or confidentiality

For More Information

Draft paper:

http://www.cs.columbia.edu/~smb/papers/codebooks.pdf

And come look at the ones I brought with me