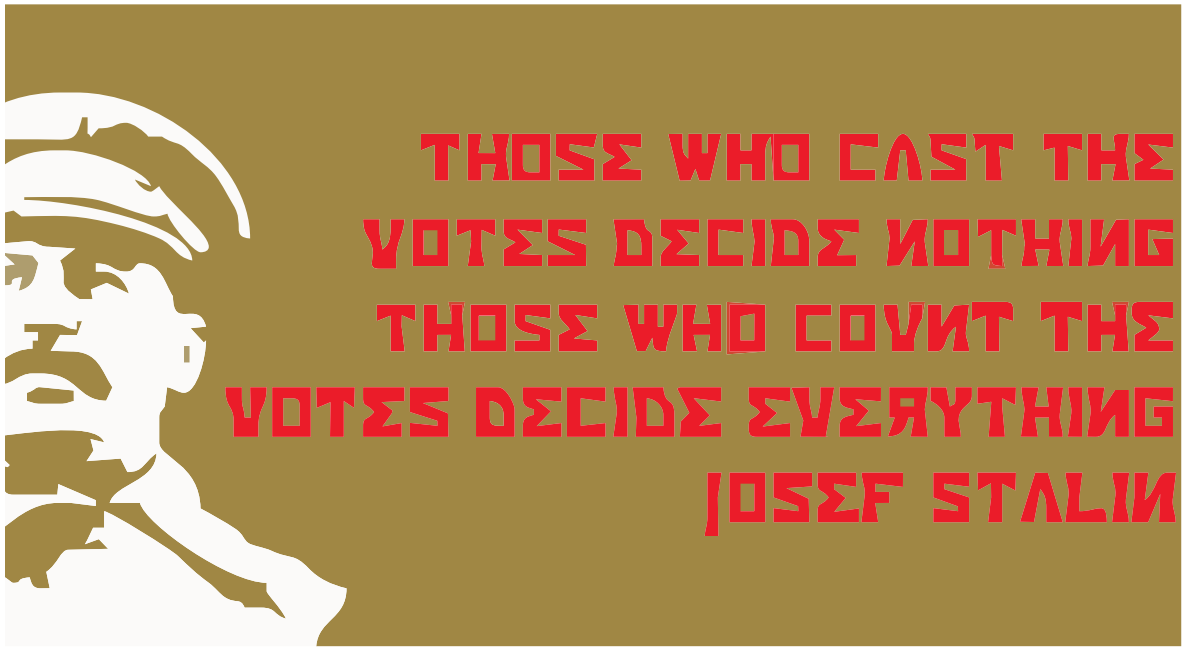
◇ Secure voting: is it possible? ◇



What problems are there with traditional voting systems (in any country)?

◇ UK Parliamentary Elections ◇

Voting procedure:

1. Turn up to the polling station, with or without your polling card.
2. Election official hands you a ballot paper, with a serial number on the top.
3. Mark an 'X' next to the candidate of your choice.
4. Put the ballot paper in the box.

Tallying procedure:

1. All ballot papers collected together at a central counting station.
2. Counters sort the votes into piles, while party officials watch.
3. Piles are counted.
4. Returning officer announces the total for each candidate.

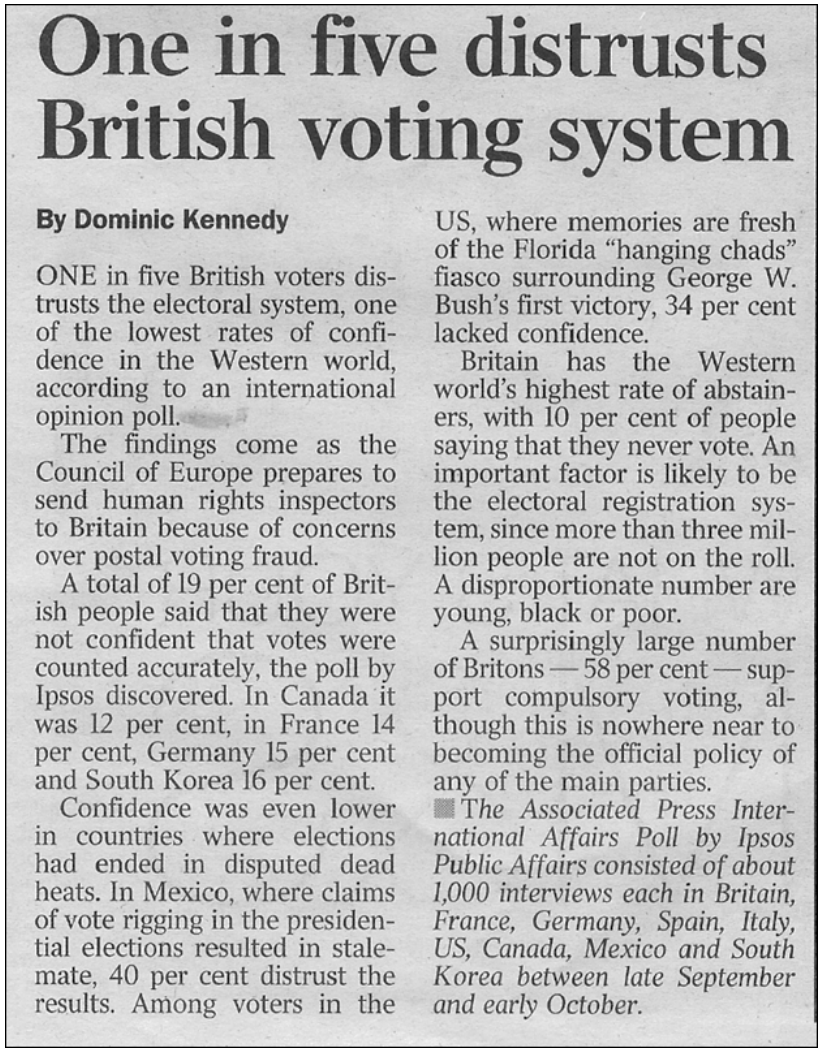
◇ Problems ◇

Coercion: ballot papers are numbered, so anyone with access to the list of voters and the ballot papers afterwards can see how you voted.

Ballot stuffing: how do you know that only real votes were counted, and that no-one introduced a load of extra votes into the ballot box?

Ballot stealing: how do you know that your vote was included in the count, and that it wasn't changed from what you wanted?

Vote counting: how do you verify that the count was conducted fairly and accurately?



One in five distrusts British voting system

By Dominic Kennedy

ONE in five British voters distrusts the electoral system, one of the lowest rates of confidence in the Western world, according to an international opinion poll.

The findings come as the Council of Europe prepares to send human rights inspectors to Britain because of concerns over postal voting fraud.

A total of 19 per cent of British people said that they were not confident that votes were counted accurately, the poll by Ipsos discovered. In Canada it was 12 per cent, in France 14 per cent, Germany 15 per cent and South Korea 16 per cent.

Confidence was even lower in countries where elections had ended in disputed dead heats. In Mexico, where claims of vote rigging in the presidential elections resulted in stalemate, 40 per cent distrust the results. Among voters in the US, where memories are fresh of the Florida "hanging chads" fiasco surrounding George W. Bush's first victory, 34 per cent lacked confidence.

Britain has the Western world's highest rate of abstainers, with 10 per cent of people saying that they never vote. An important factor is likely to be the electoral registration system, since more than three million people are not on the roll. A disproportionate number are young, black or poor.

A surprisingly large number of Britons — 58 per cent — support compulsory voting, although this is nowhere near to becoming the official policy of any of the main parties.

The Associated Press International Affairs Poll by Ipsos Public Affairs consisted of about 1,000 interviews each in Britain, France, Germany, Spain, Italy, US, Canada, Mexico and South Korea between late September and early October.

◇ Electronic voting: a solution? ◇

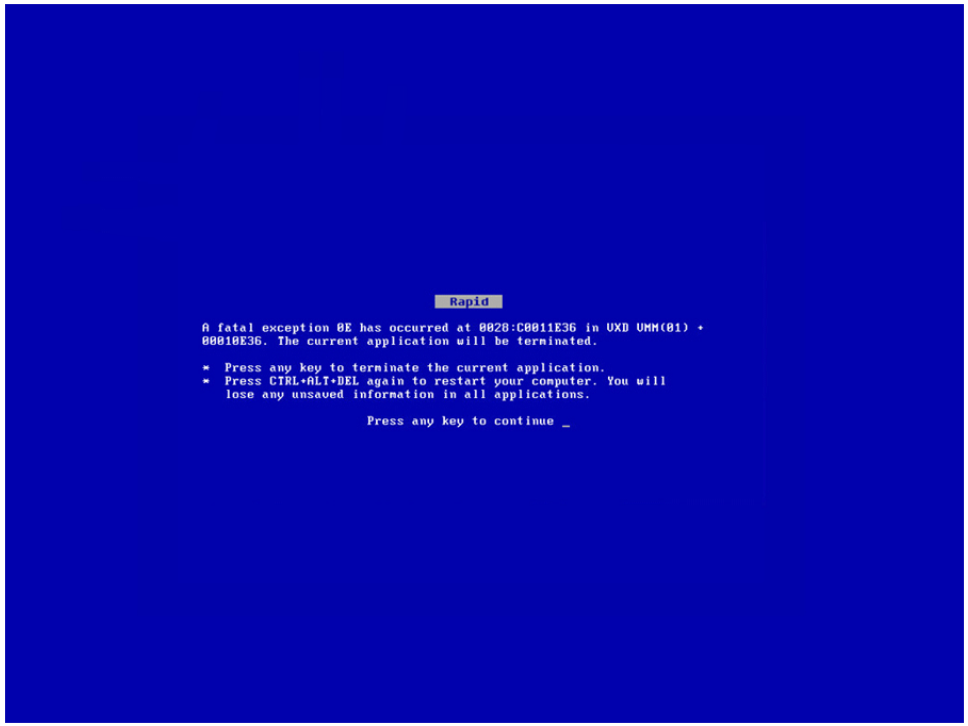
Electronic voting introduces a whole new raft of problems.

Trusting the machine: how do you know that the machine correctly recorded your vote?

Bugs: how do you know that the programmer didn't screw up somewhere?

Technology failure: what if there's a power cut?

Large-scale fraud: how can you be sure that the entire result isn't now fabricated?



◇ Desirable properties of a voting system ◇

Receipt-freeness: you should not be able to prove afterwards to a third party how you voted.

Voter verifiability: you should be able to check that your vote has been correctly included in the count, and challenge the result (without revealing your vote) if not.

Anonymity: roughly speaking, no-one should be able to tell how you voted (but why is this not quite good enough as a definition?).

Auditable tallying: you should be able to verify that the votes have been added up correctly, without any votes being lost, added or changed.

◇ ThreeBallot: a non-cryptographic solution ◇

Ron Rivest (of RSA fame) has developed a FPTP voting system that (nearly) provides for security without reliance on any cryptography at all.

Alice		**Alice**		**Alice**	
Bob		**Bob**		**Bob**	
Charlie		**Charlie**		**Charlie**	
Doug		**Doug**		**Doug**	
Erin		**Erin**		**Erin**	
	813234		933061		105212

When you go into the polling station, you are given a *multi-ballot*, containing three separate voting forms. Each contains a list of candidate names in the usual fashion, and each contains a unique ballot ID at the bottom.

The IDs have no meaning, and there is nothing to link the three IDs on the multi-ballot.

◇ Marking the ballot paper ◇

On the three ballots as a whole, you *must* vote for one candidate (your preferred candidate) twice, and everybody else once.

Alice	**X**	**Alice**		**Alice**	
Bob	**X**	**Bob**		**Bob**	**X**
Charlie		**Charlie**	**X**	**Charlie**	
Doug	**X**	**Doug**		**Doug**	
Erin		**Erin**		**Erin**	**X**
	813234		**933061**		**105212**

Whom have we voted for here?

We scan the multi-ballot into the checker, which confirms that the vote is valid. Then we tear down the perforations to separate into three ballot papers.

◇ Getting a receipt and casting the vote ◇

The individual ballot papers can now be placed into the ballot box in the usual way.

But before we do this, we choose any of the ballots we like, and have it duplicated (by machine). This duplicated ballot becomes our receipt.

Alice	
Bob	**X**
Charlie	
Doug	
Erin	**X**
	105212

What can someone tell about the vote from looking at the receipt?

◇ Tallying ◇

When voting is over, all of the ballot forms are posted up on a web bulletin board somewhere for all to see, along with a list of those who voted.

This means that we can check two important things.

Our vote: we can look on the web bulletin board to find the vote with the ID matching the one on our receipt, and check that the marks are in the right place.

If they aren't, we can kick up a fuss, but *without* revealing our vote (because the receipt doesn't tell anyone the vote).

The result: since all the ballot forms have been made public, the counting can be publicly verified.

Finding the winner is a simple case of counting who has most votes. Every candidate will receive one extra vote for each voter, but this doesn't affect who wins.

But what are the problems with this system?

◇ Problems ◇

ThreeBallot comes pretty close to providing a secure voting system with no cryptography in sight. But it does have some weaknesses.

The checker: it is difficult to see how we could *prove* that the checker contains no dodgy equipment to record our vote.

Changing after checking: a voter who can add more crosses after having the ballot checked can give extra votes.

Not submitting all ballots: we would need a mechanism to ensure that the voter submits all three ballot papers.

Dodgy receipts: we need something to stop voters from constructing faked receipts to 'prove' that their vote is absent or wrong.

Reconstructing multi-ballots: can we be sure that the printing process didn't keep records of which ballots went with which others? And might a ballot form have only two others that it could be matched with to create a valid vote?

◇ The ThreePattern attack ◇

Although a coercer cannot gain anything from forcing you to produce a receipt filled out in a particular way, he might force you to fill in a multi-ballot in a particular way.

Alice	**X**	**Alice**		**Alice**	
Bob	**X**	**Bob**		**Bob**	**X**
Charlie		**Charlie**	**X**	**Charlie**	
Doug	**X**	**Doug**		**Doug**	
Erin		**Erin**		**Erin**	**X**
Fred	**X**	**Fred**		**Fred**	
George	**X**	**George**		**George**	
Helen		**Helen**		**Helen**	**X**
Isobel		**Isobel**	**X**	**Isobel**	
Judith		**Judith**		**Judith**	**X**
	813234		**933061**		**105212**

What if he tells you to fill it in like this, and bring the middle column back as a receipt?

◇ The Short Ballot Assumption ◇

The *short ballot assumption*: every possible ballot paper will with high probability turn up a large number of times (or, to be more precise, a number of times that is difficult to predict).

This protects against many attacks like the ThreePattern attack: if the short ballot assumption holds, the pattern dictated to you on each individual ballot will appear on the web site anyway.

As we will see, this depends partly on the tallying method and partly on the mechanics of the voting system.

◇ VAV ◇

With n candidates, there are 2^n ways of filling in an individual ballot paper. Even small(ish) values of n will fail the short ballot assumption.

	Vote		Anti-vote		Vote
Alice		**Alice**		**Alice**	
Bob		**Bob**		**Bob**	
Charlie		**Charlie**		**Charlie**	
Doug		**Doug**		**Doug**	
Erin		**Erin**		**Erin**	
	813234		933061		105212

VAV is a variant on ThreeBallot. It works the same, except that you cast two normal votes (green), and one anti-vote (red) that cancels one of your votes.

What are the advantages of this?

◇ Advantages of VAV ◇

Three major advantages:

1. It's much more usable for the average voter
2. It's more likely to satisfy the short ballot assumption
3. It can be used for any tallying method (including preferential voting systems)

It is worth noting that both these systems are compatible with allowing lazy voters to cast a normal ballot if they want to (as long as their ballots are indistinguishable from individual ballots from ThreeBallot or VAV).

◇ Twin ◇

Part of the design goal has been to ensure that your receipt reveals no information about your vote. There is one other way of achieving this: we give you a copy of **someone else's** vote.

Twin works roughly like this:

1. Fill out a normal (single) ballot, in the usual way. It has a random ID at the bottom.
2. Get given a copy of a random ballot cast by a previous voter. (Note that this may have been copied for someone else too.)
3. Put your ballot into the ballot box.
4. Check the receipt you've been given on the bulletin board.

Can you see how this helps? Are there any problems? Do we still need the SBA?

◇ Scratch strip IDs ◇

There is still an issue if you can remember or copy out your ID. We can mitigate this somewhat:

1. Fill out a normal (single) ballot, in the usual way. It has a random ID at the bottom, covered by a scratch strip.
2. Get given a copy of a random ballot cast by a previous voter.
3. Put your ballot into the ballot box. The box has some mechanism for scratching the strip off as the ballot goes in.
4. Check the receipt you've been given on the bulletin board.

How does that help? Can we make the box translucent so you can see what's going on but not read the ID?

◇ Conclusion ◇

We **almost** don't need crypto!

ThreeBallot: almost secure enough, but has some problems. Main ones: constructing the checker would be tricky; it's unusable for the uneducated voter (is that a good thing or a bad thing. . . ?)

VAV: better security, better usability, but still problems with the checker, and still not very grandma-friendly.

Twin: pretty close, and probably could be used in practice.

But maybe we can do even better with crypto.